



Security Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)

First Published: January 29, 2013

Last Modified: October 07, 2013

Americas Headquarters

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

Text Part Number: OL-28525-02



CONTENTS

Preface

Preface **xxiii**

Audience **xxiii**

Document Conventions **xxiii**

Related Documentation **xxiv**

Changes to This Document **xxv**

Obtaining Documentation and Submitting a Service Request **xxv**

CHAPTER 1

Using the Command-Line Interface **1**

Information About Using the Command-Line Interface **1**

Command Modes **1**

Understanding Abbreviated Commands **3**

No and Default Forms of Commands **4**

CLI Error Messages **4**

Configuration Logging **4**

Using the Help System **5**

How to Use the CLI to Configure Features **6**

Configuring the Command History **6**

 Changing the Command History Buffer Size **6**

 Recalling Commands **7**

 Disabling the Command History Feature **7**

Enabling and Disabling Editing Features **8**

 Editing Commands Through Keystrokes **8**

 Editing Command Lines That Wrap **10**

Searching and Filtering Output of show and more Commands **11**

Accessing the CLI Through a Console Connection or Through Telnet **11**

CHAPTER 2

Using the Web Graphical User Interface **13**

Prerequisites for Using the Web GUI	13
Information About Using The Web GUI	13
Web GUI Features	13
Connecting the Console Port of the Controller	15
Logging On to the Web GUI	15
Enabling Web and Secure Web Modes	15
Configuring the Controller Web GUI	16

CHAPTER 3**Preventing Unauthorized Access 21**

Finding Feature Information	21
Preventing Unauthorized Access	21

CHAPTER 4**Controlling Switch Access with Passwords and Privilege Levels 23**

Finding Feature Information	23
Restrictions for Controlling Switch Access with Passwords and Privileges	23
Information About Passwords and Privilege Levels	24
Default Password and Privilege Level Configuration	24
Additional Password Security	24
Password Recovery	25
Terminal Line Telnet Configuration	25
Username and Password Pairs	25
Privilege Levels	26
How to Control Switch Access with Passwords and Privilege Levels	26
Setting or Changing a Static Enable Password	26
Protecting Enable and Enable Secret Passwords with Encryption	28
Disabling Password Recovery	30
Setting a Telnet Password for a Terminal Line	32
Configuring Username and Password Pairs	34
Setting the Privilege Level for a Command	36
Changing the Default Privilege Level for Lines	38
Logging into and Exiting a Privilege Level	39
Monitoring Switch Access	40
Configuration Examples for Setting Passwords and Privilege Levels	40
Example: Setting or Changing a Static Enable Password	40
Example: Protecting Enable and Enable Secret Passwords with Encryption	41

Example: Setting a Telnet Password for a Terminal Line	41
Example: Setting the Privilege Level for a Command	41
Additional References	41

CHAPTER 5**Configuring TACACS+ 43**

Finding Feature Information	43
Prerequisites for Controlling Switch Access with Terminal Access Controller Access Control System Plus (TACACS+)	43
Information About TACACS+	45
TACACS+ and Switch Access	45
TACACS+ Overview	45
TACACS+ Operation	47
Method List	48
TACACS+ Configuration Options	48
TACACS+ Login Authentication	48
TACACS+ Authorization for Privileged EXEC Access and Network Services	48
TACACS+ Accounting	49
Default TACACS+ Configuration	49
How to Configure TACACS+	49
Identifying the TACACS+ Server Host and Setting the Authentication Key	49
Configuring TACACS+ Login Authentication	51
Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services	54
Starting TACACS+ Accounting	56
Establishing a Session with a Router if the AAA Server is Unreachable	57
Monitoring TACACS+	58
Additional References	58

CHAPTER 6**Configuring RADIUS 61**

Finding Feature Information	61
Prerequisites for Controlling SwitchController Access with RADIUS	61
Restrictions for Controlling SwitchController Access with RADIUS	62
Information about RADIUS	63
RADIUS and Switch Access	63
RADIUS Overview	63
RADIUS Operation	64

RADIUS Change of Authorization	65
Change-of-Authorization Requests	65
RFC 5176 Compliance	66
CoA Request Response Code	67
Session Identification	67
CoA ACK Response Code	68
CoA NAK Response Code	68
CoA Request Commands	68
Session Reauthentication	68
Session Reauthentication in a Switch Stack	69
Session Termination	69
CoA Disconnect-Request	69
CoA Request: Disable Host Port	70
CoA Request: Bounce-Port	70
Stacking Guidelines for Session Termination	71
Stacking Guidelines for CoA-Request Bounce-Port	71
Stacking Guidelines for CoA-Request Disable-Port	71
Default RADIUS Configuration	71
RADIUS Server Host	72
RADIUS Login Authentication	72
AAA Server Groups	73
AAA Authorization	73
RADIUS Accounting	73
Vendor-Specific RADIUS Attributes	74
Vendor-Proprietary RADIUS Server Communication	74
How to Configure RADIUS	74
Identifying the RADIUS Server Host	74
Configuring RADIUS Login Authentication	77
Defining AAA Server Groups	79
Configuring RADIUS Authorization for User Privileged Access and Network Services	82
Starting RADIUS Accounting	84
Configuring Settings for All RADIUS Servers	86
Configuring the Controller to Use Vendor-Specific RADIUS Attributes	87
Configuring the Controller for Vendor-Proprietary RADIUS Server Communication	89
Configuring CoA on the Controller	90

Monitoring CoA Functionality	93
Configuration Examples for Controlling Switch Access with RADIUS	94
Examples: Identifying the RADIUS Server Host	94
Example: Using Two Different RADIUS Group Servers	94
Examples: Configuring the Switch to Use Vendor-Specific RADIUS Attributes	95
Example: Configuring the Switch for Vendor-Proprietary RADIUS Server Communication	95
Additional References	96

CHAPTER 7
Configuring Kerberos 99

Finding Feature Information	99
Prerequisites for Controlling Switch Access with Kerberos	99
Information about Kerberos	100
Kerberos and Switch Access	100
Kerberos Overview	100
Kerberos Operation	103
Authenticating to a Boundary Switch	103
Obtaining a TGT from a KDC	103
Authenticating to Network Services	104
How to Configure Kerberos	104
Monitoring the Kerberos Configuration	104
Additional References	104

CHAPTER 8
Configuring Local Authentication and Authorization 107

Finding Feature Information	107
How to Configure Local Authentication and Authorization	107
Configuring the Switch for Local Authentication and Authorization	107
Monitoring Local Authentication and Authorization	110
Additional References	110

CHAPTER 9
Configuring Local Authentication 113

Information About Local Web Authentication	113
Restrictions for Local Web Authentication	114
Configuring Local Web Authentication	115
Configuring Local Web Authentication for Local Net Users Using AAA (CLI)	115
Configuring Local Web Authentication Using RADIUS Server (CLI)	116

Configuring Local Web Authentication Using RADIUS Server (GUI)	117
Configuring Guest Users for Local Web Authentication (CLI)	117
Configuring Guest Users for Local Web Authentication (GUI)	118
Configuring a Parameter Map for Local Web Authentication (CLI)	119
Configuring a Parameter Map and Method List for Local Web Authentication (GUI)	122
Configuring Local Web Authentication on a WLAN (CLI)	124
Configuring Local Web Authentication on a WLAN (GUI)	126
Monitoring Local Web Authentication	126
Examples: Local Web Authentication Configuration	126
Additional References for Configuring the Local Web Authentication Configuration	128
Feature History for Performing Local Web Authentication Configuration	129

CHAPTER 10**Configuring Secure Shell (SSH) 131**

Finding Feature Information	131
Prerequisites for Configuring the Switch for Secure Shell (SSH) and Secure Copy Protocol (SCP)	131
Restrictions for Configuring the SwitchController for SSH	132
Information about SSH	132
SSH and Switch Access	133
SSH Servers, Integrated Clients, and Supported Versions	133
SSH Configuration Guidelines	133
Secure Copy Protocol Overview	134
Secure Copy Protocol	134
How to Configure SSH	135
Setting Up the SwitchController to Run SSH	135
Configuring the SSH Server	136
Monitoring the SSH Configuration and Status	139
Additional References	139

CHAPTER 11**Configuring Secure Socket Layer HTTP 141**

Finding Feature Information	141
Information about Secure Sockets Layer (SSL) HTTP	141
Secure HTTP Servers and Clients Overview	141
Certificate Authority Trustpoints	142
CipherSuites	143

Default SSL Configuration	144
SSL Configuration Guidelines	144
How to Configure Secure HTTP Servers and Clients	144
Configuring a CA Trustpoint	144
Configuring the Secure HTTP Server	146
Configuring the Secure HTTP Client	149
Monitoring Secure HTTP Server and Client Status	150
Additional References	151

CHAPTER 12

Configuring IPv4 ACLs	153
Finding Feature Information	153
Prerequisites for Configuring Network Security with ACLs	153
Restrictions for Configuring Network Security with ACLs	154
Information about Network Security with ACLs	155
ACL Overview	155
Access Control Entries	156
ACL Supported Types	156
Supported ACLs	156
ACL Precedence	156
Port ACLs	157
Router ACLs	158
VLAN Maps	159
ACEs and Fragmented and Unfragmented Traffic	159
Example: ACES and Fragmented and Unfragmented Traffic	160
ACLs and Switch Stacks	160
Active Switch and ACL Functions	161
Stack Member and ACL Functions	161
Active Switch Failure and ACLs	161
Standard and Extended IPv4 ACLs	161
IPv4 ACL Switch Unsupported Features	161
Access List Numbers	162
Numbered Standard IPv4 ACLs	163
Numbered Extended IPv4 ACLs	163
Named IPv4 ACLs	164
ACL Logging	164

Hardware and Software Treatment of IP ACLs	165
VLAN Map Configuration Guidelines	166
VLAN Maps with Router ACLs	167
VLAN Maps and Router ACL Configuration Guidelines	167
VACL Logging	168
Time Ranges for ACLs	168
IPv4 ACL Interface Considerations	169
How to Configure ACLs	169
Configuring IPv4 ACLs	169
Creating a Numbered Standard ACL	170
Creating a Numbered Extended ACL	171
Creating Named Standard ACLs	175
Creating Extended Named ACLs	176
Configuring Time Ranges for ACLs	178
Applying an IPv4 ACL to a Terminal Line	180
Applying an IPv4 ACL to an Interface	182
Creating Named MAC Extended ACLs	183
Applying a MAC ACL to a Layer 2 Interface	185
Configuring VLAN Maps	187
Creating a VLAN Map	189
Applying a VLAN Map to a VLAN	191
Monitoring IPv4 ACLs	192
Configuration Examples for ACLs	193
Examples: Using Time Ranges with ACLs	193
Examples: Including Comments in ACLs	194
IPv4 ACL Configuration Examples	194
ACLs in a Small Networked Office	195
Examples: ACLs in a Small Networked Office	195
Example: Numbered ACLs	196
Examples: Extended ACLs	196
Examples: Named ACLs	197
Examples: Time Range Applied to an IP ACL	198
Examples: Commented IP ACL Entries	198
Examples: ACL Logging	198
Configuration Examples for ACLs and VLAN Maps	200

Example: Creating an ACL and a VLAN Map to Deny a Packet	200
Example: Creating an ACL and a VLAN Map to Permit a Packet	200
Example: Default Action of Dropping IP Packets and Forwarding MAC Packets	200
Example: Default Action of Dropping MAC Packets and Forwarding IP Packets	201
Example: Default Action of Dropping All Packets	201
Configuration Examples for Using VLAN Maps in Your Network	202
Example: Wiring Closet Configuration	202
Example: Restricting Access to a Server on Another VLAN	203
Example: Denying Access to a Server on Another VLAN	203
Configuration Examples of Router ACLs and VLAN Maps Applied to VLANs	204
Example: ACLs and Switched Packets	204
Example: ACLs and Bridged Packets	204
Example: ACLs and Routed Packets	205
Example: ACLs and Multicast Packets	206
Additional References	206

CHAPTER 13
Configuring DHCP 209

Finding Feature Information	209
Information About DHCP	209
DHCP Server	209
DHCP Relay Agent	209
DHCP Snooping	210
Option-82 Data Insertion	211
Cisco IOS DHCP Server Database	214
DHCP Snooping Binding Database	214
DHCP Snooping and Switch Stacks	216
How to Configure DHCP Features	216
Default DHCP Snooping Configuration	216
DHCP Snooping Configuration Guidelines	217
Configuring the DHCP Server	217
DHCP Server and Switch Stacks	217
Configuring the DHCP Relay Agent	218
Specifying the Packet Forwarding Address	219
Prerequisites for Configuring DHCP Snooping and Option 82	222
Enabling DHCP Snooping and Option 82	223

Enabling the Cisco IOS DHCP Server Database	227
Monitoring DHCP Snooping Information	227
Configuring DHCP Server Port-Based Address Allocation	228
DHCP Server Port-Based Address Allocation	228
Default Port-Based Address Allocation Configuration	228
Port-Based Address Allocation Configuration Guidelines	228
Enabling the DHCP Snooping Binding Database Agent	229
Enabling DHCP Server Port-Based Address Allocation	231
Monitoring DHCP Server Port-Based Address Allocation	233
Additional References	233

CHAPTER 14

Configuring IP Source Guard	235
Finding Feature Information	235
Information About IP Source Guard	235
IP Source Guard	235
IP Source Guard for Static Hosts	236
IP Source Guard Configuration Guidelines	237
How to Configure IP Source Guard	238
Enabling IP Source Guard	238
Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port	240
Monitoring IP Source Guard	242
Additional References	242

CHAPTER 15

Configuring Dynamic ARP Inspection	245
Finding Feature Information	245
Restrictions for Dynamic ARP Inspection	245
Understanding Dynamic ARP Inspection	247
Interface Trust States and Network Security	248
Rate Limiting of ARP Packets	249
Relative Priority of ARP ACLs and DHCP Snooping Entries	250
Logging of Dropped Packets	250
Default Dynamic ARP Inspection Configuration	250
Relative Priority of ARP ACLs and DHCP Snooping Entries	251
Configuring ARP ACLs for Non-DHCP Environments	251
Configuring Dynamic ARP Inspection in DHCP Environments	254

Limiting the Rate of Incoming ARP Packets	257
Performing Dynamic ARP Inspection Validation Checks	259
Monitoring DAI	261
Verifying the DAI Configuration	262
Additional References	262

CHAPTER 16

Configuring IEEE 802.1x Port-Based Authentication	265
Finding Feature Information	265
Information About 802.1x Port-Based Authentication	265
Port-Based Authentication Process	266
Port-Based Authentication Initiation and Message Exchange	268
Authentication Manager for Port-Based Authentication	270
Port-Based Authentication Methods	270
Per-User ACLs and Filter-Ids	271
Port-Based Authentication Manager CLI Commands	272
Ports in Authorized and Unauthorized States	273
Port-Based Authentication and Switch Stacks	274
802.1x Host Mode	275
802.1x Multiple Authentication Mode	275
Multi-auth Per User VLAN assignment	276
Limitation in Multi-auth Per User VLAN assignment	277
MAC Move	277
MAC Replace	278
802.1x Accounting	278
802.1x Accounting Attribute-Value Pairs	279
802.1x Readiness Check	280
Switch-to-RADIUS-Server Communication	280
802.1x Authentication with VLAN Assignment	280
802.1x Authentication with Per-User ACLs	282
802.1x Authentication with Downloadable ACLs and Redirect URLs	283
Cisco Secure ACS and Attribute-Value Pairs for the Redirect URL	285
Cisco Secure ACS and Attribute-Value Pairs for Downloadable ACLs	285
VLAN ID-based MAC Authentication	286
802.1x Authentication with Guest VLAN	286
802.1x Authentication with Restricted VLAN	287

802.1x Authentication with Inaccessible Authentication Bypass	288
Inaccessible Authentication Bypass Support on Multiple-Authentication Ports	288
Inaccessible Authentication Bypass Authentication Results	288
Inaccessible Authentication Bypass Feature Interactions	289
802.1x Critical Voice VLAN	290
802.1x User Distribution	290
802.1x User Distribution Configuration Guidelines	291
IEEE 802.1x Authentication with Voice VLAN Ports	291
IEEE 802.1x Authentication with Port Security	292
IEEE 802.1x Authentication with Wake-on-LAN	292
IEEE 802.1x Authentication with MAC Authentication Bypass	292
Network Admission Control Layer 2 IEEE 802.1x Validation	293
Flexible Authentication Ordering	294
Open1x Authentication	294
Multidomain Authentication	295
802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT)	296
Voice Aware 802.1x Security	298
Common Session ID	298
How to Configure 802.1x Port-Based Authentication	299
Default 802.1x Authentication Configuration	299
802.1x Authentication Configuration Guidelines	300
802.1x Authentication	300
VLAN Assignment, Guest VLAN, Restricted VLAN, and Inaccessible Authentication Bypass	301
MAC Authentication Bypass	302
Maximum Number of Allowed Devices Per Port	302
Configuring 802.1x Readiness Check	302
Configuring Voice Aware 802.1x Security	304
Configuring 802.1x Violation Modes	306
Configuring 802.1x Authentication	308
Configuring 802.1x Port-Based Authentication	309
Configuring the Switch-to-RADIUS-Server Communication	311
Configuring the Host Mode	313
Configuring Periodic Re-Authentication	314

Changing the Quiet Period	315
Changing the Switch-to-Client Retransmission Time	317
Setting the Switch-to-Client Frame-Retransmission Number	318
Setting the Re-Authentication Number	319
Enabling MAC Move	321
Enabling MAC Replace	322
Configuring 802.1x Accounting	323
Configuring a Guest VLAN	325
Configuring a Restricted VLAN	326
Configuring Number of Authentication Attempts on a Restricted VLAN	328
Configuring 802.1x Inaccessible Authentication Bypass with Critical Voice VLAN	330
Example of Configuring Inaccessible Authentication Bypass	333
Configuring 802.1x Authentication with WoL	334
Configuring MAC Authentication Bypass	335
Formatting a MAC Authentication Bypass Username and Password	336
Configuring 802.1x User Distribution	337
Example of Configuring VLAN Groups	338
Configuring NAC Layer 2 802.1x Validation	339
Configuring an Authenticator Switch with NEAT	341
Configuring a Supplicant Switch with NEAT	343
Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs	345
Configuring Downloadable ACLs	346
Configuring a Downloadable Policy	347
Configuring VLAN ID-based MAC Authentication	350
Configuring Flexible Authentication Ordering	351
Configuring Open1x	352
Disabling 802.1x Authentication on the Port	355
Resetting the 802.1x Authentication Configuration to the Default Values	356
Monitoring 802.1x Statistics and Status	357
Additional References	358

CHAPTER 17
Configuring Web-Based Authentication 361

Finding Feature Information	361
Information About Web-Based Authentication	361
Device Roles	362

Host Detection	362
Session Creation	363
Authentication Process	363
Local Web Authentication Banner	364
Web Authentication Customizable Web Pages	366
Guidelines	366
Authentication Proxy Web Page Guidelines	368
Redirection URL for Successful Login Guidelines	369
Web-based Authentication Interactions with Other Features	369
Port Security	369
LAN Port IP	369
Gateway IP	370
ACLs	370
Context-Based Access Control	370
EtherChannel	370
How to Configure Web-Based Authentication	370
Default Web-Based Authentication Configuration	370
Web-Based Authentication Configuration Guidelines and Restrictions	371
Configuring the Authentication Rule and Interfaces	372
Configuring AAA Authentication	374
Configuring Switch-to-RADIUS-Server Communication	376
Configuring the HTTP Server	378
Customizing the Authentication Proxy Web Pages	379
Specifying a Redirection URL for Successful Login	381
Configuring the Web-Based Authentication Parameters	382
Configuring a Web Authentication Local Banner	383
Removing Web-Based Authentication Cache Entries	385
Sample Web Authentication Login HTML	386
Monitoring Web-Based Authentication Status	387

CHAPTER 18

Configuring Port-Based Traffic Control	389
Finding Feature Information	390
Information About Storm Control	390
Storm Control	390
How Traffic Activity is Measured	390

Traffic Patterns	391
How to Configure Storm Control	392
Configuring Storm Control and Threshold Levels	392
Configuring Small-Frame Arrival Rate	394
Monitoring Storm Control	397
Where to Go Next	397
Feature Information	397
Information About Protected Ports	397
Protected Ports	397
Default Protected Port Configuration	398
Protected Ports Guidelines	398
How to Configure Protected Ports	398
Configuring a Protected Port	398
Monitoring Protected Ports	400
Where to Go Next	400
Feature Information	400
Information About Port Blocking	400
Port Blocking	400
How to Configure Port Blocking	401
Blocking Flooded Traffic on an Interface	401
Monitoring Port Blocking	403
Where to Go Next	403
Feature Information	403
Prerequisites for Port Security	403
Restrictions for Port Security	403
Information About Port Security	404
Port Security	404
Types of Secure MAC Addresses	404
Sticky Secure MAC Addresses	404
Security Violations	405
Port Security Aging	406
Port Security and Switch Stacks	406
Default Port Security Configuration	406
Port Security Configuration Guidelines	407
How to Configure Port Security	408

Enabling and Configuring Port Security	408
Enabling and Configuring Port Security Aging	413
Configuring Port Security and Private VLANs	415
Monitoring Port Security	417
Configuration Examples for Port Security	417
Where to Go Next	418
Feature Information	418
Information About Protocol Storm Protection	418
Protocol Storm Protection	418
Default Protocol Storm Protection Configuration	419
How to Configure Protocol Storm Protection	419
Enabling Protocol Storm Protection	419
Monitoring Protocol Storm Protection	421

CHAPTER 19

Configuring Cisco TrustSec	423
Information about Cisco TrustSec	423
Finding Feature Information	423
Cisco TrustSec Features	424
Feature Information for Cisco TrustSec	426

CHAPTER 20

Configuring IPv6 First Hop Security	427
Finding Feature Information	427
Prerequisites for First Hop Security in IPv6	427
Restrictions for First Hop Security in IPv6	428
Information about First Hop Security in IPv6	428
How to Configure an IPv6 Snooping Policy	432
How to Attach an IPv6 Snooping Policy to an Interface	434
How to Attach an IPv6 Snooping Policy to a Layer 2 EtherChannel Interface	435
How to Attach an IPv6 Snooping Policy to VLANs Globally	436
How to Configure the IPv6 Binding Table Content	437
How to Configure an IPv6 Neighbor Discovery Inspection Policy	439
How to Attach an IPv6 Neighbor Discovery Inspection Policy to an Interface	441
How to Attach an IPv6 Neighbor Discovery Inspection Policy to a Layer 2 EtherChannel Interface	442
How to Attach an IPv6 Neighbor Discovery Inspection Policy to VLANs Globally	443

How to Configure an IPv6 Router Advertisement Guard Policy	444
How to Attach an IPv6 Router Advertisement Guard Policy to an Interface	446
How to Attach an IPv6 Router Advertisement Guard Policy to a Layer 2 EtherChannel Interface	448
How to Attach an IPv6 Router Advertisement Guard Policy to VLANs Globally	449
How to Configure an IPv6 DHCP Guard Policy	450
How to Attach an IPv6 DHCP Guard Policy to an Interface or a VLAN on an Interface	452
How to Attach an IPv6 DHCP Guard Policy to a Layer 2 EtherChannel Interface	453
How to Attach an IPv6 DHCP Guard Policy to VLANs Globally	454
Additional References	455

CHAPTER 21
Managing Rogue Devices 457

Finding Feature Information	457
Information About Rogue Devices	457
How to Configure Rogue Detection	462
Configuring Rogue Detection (CLI)	462
Configuring Rogue Detection (GUI)	463
Monitoring Rogue Detection	464
Examples: Rogue Detection Configuration	464
Additional References for Rogue Detection	465
Feature History and Information For Performing Rogue Detection Configuration	466

CHAPTER 22
Classifying Rogue Access Points 467

Finding Feature Information	467
Information About Classifying Rogue Access Points	467
Restrictions for Classifying Rogue Access Points	470
How to Classify Rogue Access Points	471
Configuring Rogue Classification Rules (CLI)	471
Configuring Rogue Classification Rules (GUI)	473
Viewing and Classifying Rogue Devices (GUI)	475
Examples: Classifying Rogue Access Points	477
Additional References for Classifying Rogue Access Points	478
Feature History and Information For Classifying Rogue Access Points	479

CHAPTER 23
Configuring wIPS 481

Finding Feature Information	481
Information About wIPS	481
How to Configure wIPS on an Access Point	488
Configuring wIPS on an Access Point (CLI)	488
Configuring wIPS on an Access Point (GUI)	489
Monitoring wIPS Information	490
Examples: wIPS Configuration	490
Additional References for Configuring wIPS	490
Feature History for Performing wIPS Configuration	491

CHAPTER 24

Configuring Wireless Guest Access	493
Finding Feature Information	493
Prerequisites for Guest Access	493
Restrictions for Guest Access	494
Information about Wireless Guest Access	494
Fast Secure Roaming	494
How to Configure Guest Access	495
Creating a Lobby Administrator Account	495
Configuring Guest User Accounts	496
Configuring Mobility Agent (MA)	497
Configuring Mobility Controller	499
Obtaining a Web Authentication Certificate	500
Displaying a Web Authentication Certificate	501
Choosing the Default Web Authentication Login Page	501
Choosing a Customized Web Authentication Login Page from an External Web Server	503
Assigning Login, Login Failure, and Logout Pages per WLAN	505
Configuring AAA-Override	506
Configuring Client Load Balancing	507
Configuring Preauthentication ACL	508
Configuring IOS ACL Definition	509
Configuring Webpassthrough	510
Configuration Examples for Guest Access	511
Example: Creating a Lobby Ambassador Account	511
Example: Obtaining Web Authentication Certificate	511
Example: Displaying a Web Authentication Certificate	512

Example: Configuring Guest User Accounts	513
Example: Configuring Mobility Controller	513
Example: Choosing the Default Web Authentication Login Page	514
Example: Choosing a Customized Web Authentication Login Page from an External Web Server	515
Example: Assigning Login, Login Failure, and Logout Pages per WLAN	515
Example: Configuring AAA-Override	515
Example: Configuring Client Load Balancing	516
Example: Configuring Preauthentication ACL	516
Example: Configuring IOS ACL Definition	516
Example: Configuring Webpassthrough	516
Additional References for Guest Access	517
Feature History and Information for Guest Access	518

CHAPTER 25

Configuring Intrusion Detection System	519
Finding Feature Information	519
Information About Intrusion Detection System	519
How to Configure Intrusion Detection System	520
Configuring IDS Sensors	520
Monitoring Intrusion Detection System	521



Preface

This book describes configuration information and examples for security management on the switch.

- [Audience](#), page xxiii
- [Document Conventions](#), page xxiii
- [Related Documentation](#), page xxiv
- [Changes to This Document](#), page xxv
- [Obtaining Documentation and Submitting a Service Request](#), page xxv

Audience

This guide is for the networking professional managing the Catalyst 3850 switch, hereafter referred to as the switch module. Before using this guide, you should have experience working with the Cisco IOS software and be familiar with the concepts and terminology of Ethernet and local area networking.

Document Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

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

Interactive examples use these conventions:

- Terminal sessions and system displays are in screen font.

- Information you enter is in boldface screen font
- Nonprinting characters, such as passwords or tabs, are in angle brackets (<>).

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

**Note**

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

Reader Alert Conventions

This document uses 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**

Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.

Related Documentation

**Note**

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

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

Changes to This Document

This table lists the technical changes made to this document since it was first printed.

Table 1: Changes to This Document

Revision	Date	Change Summary
OL-xxxxx-01	July 2012	Initial release of this document.

Obtaining Documentation and Submitting a Service Request

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

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>

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



Using the Command-Line Interface

- [Information About Using the Command-Line Interface, page 1](#)
- [How to Use the CLI to Configure Features, page 6](#)

Information About Using the Command-Line Interface

Command Modes

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

You can start a CLI session through a console connection, through Telnet, a SSH, or by using the browser.

When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the controller reboots.

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

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the controller reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

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

Table 2: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	SwitchController>	Enter logout or quit .	Use this mode to <ul style="list-style-type: none"> • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the enable command.	SwitchController#	Enter disable to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode. Use this mode to execute privilege EXEC commands for access points. These commands are not part of the running config of the controller, they are sent to the IOS config of the access point.
Global configuration	While in privileged EXEC mode, enter the configure command.	SwitchController(config)#	To exit to privileged EXEC mode, enter exit or end , or press Ctrl-Z .	Use this mode to configure parameters that apply to the entire controller. Use this mode to configure access point commands that are part of the running config of the controller.
VLAN configuration	While in global configuration mode, enter the vlan <i>vlan-id</i> command.	SwitchController(config-vlan)#		

Mode	Access Method	Prompt	Exit Method	About This Mode
			To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the controller startup configuration file.
Interface configuration	While in global configuration mode, enter the interface command (with a specific interface).	SwitchController(config-if)#	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the Ethernet ports.
Line configuration	While in global configuration mode, specify a line with the line vty or line console command.	SwitchController(config-line)#	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the terminal line.

Understanding Abbreviated Commands

You need to enter only enough characters for the controller to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
SwitchController# show conf
```

No and Default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to reenable a disabled feature or to enable a feature that is disabled by default.

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

CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your controller.

Table 3: Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for your controller to recognize the command.	Reenter the command followed by a question mark (?) without any space between the command and the question mark. The possible keywords that you can enter with the command appear.
% Incomplete command.	You did not enter all of the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
% Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Configuration Logging

You can log and view changes to the controller configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous

notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.



Note Only CLI or HTTP changes are logged.

Using the Help System

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

SUMMARY STEPS

1. **help**
2. *abbreviated-command-entry ?*
3. *abbreviated-command-entry <Tab>*
4. **?**
5. *command ?*
6. *command keyword ?*

DETAILED STEPS

	Command or Action	Purpose
Step 1	help Example: SwitchController# help	Obtains a brief description of the help system in any command mode.
Step 2	<i>abbreviated-command-entry ?</i> Example: SwitchController# di? dir disable disconnect	Obtains a list of commands that begin with a particular character string.
Step 3	<i>abbreviated-command-entry <Tab></i> Example: SwitchController# sh conf<tab> SwitchController# show configuration	Completes a partial command name.
Step 4	? Example: SwitchController> ?	Lists all commands available for a particular command mode.

	Command or Action	Purpose
Step 5	<p><i>command ?</i></p> <p>Example: SwitchController> show ?</p>	Lists the associated keywords for a command.
Step 6	<p><i>command keyword ?</i></p> <p>Example: SwitchController(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet</p>	Lists the associated arguments for a keyword.

How to Use the CLI to Configure Features

Configuring the Command History

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

Changing the Command History Buffer Size

By default, the controller records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. This procedure is optional.

SUMMARY STEPS

1. **terminal history** [*size number-of-lines*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>terminal history [<i>size number-of-lines</i>]</p> <p>Example: SwitchController# terminal history size 200</p>	Changes the number of command lines that the controller records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256.

Recalling Commands

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



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

SUMMARY STEPS

1. **Ctrl-P** or use the **up arrow** key
2. **Ctrl-N** or use the **down arrow** key
3. **show history**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Ctrl-P or use the up arrow key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Step 2	Ctrl-N or use the down arrow key	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.
Step 3	show history Example: SwitchController# show history	Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the terminal history global configuration command and the history line configuration command.

Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. This procedure is optional.

SUMMARY STEPS

1. **terminal no history**

DETAILED STEPS

	Command or Action	Purpose
Step 1	terminal no history Example: SwitchController# terminal no history	Disables the feature during the current terminal session in privileged EXEC mode.

Enabling and Disabling Editing Features

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

SUMMARY STEPS

1. terminal editing
2. terminal no editing

DETAILED STEPS

	Command or Action	Purpose
Step 1	terminal editing Example: SwitchController# terminal editing	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.
Step 2	terminal no editing Example: SwitchController# terminal no editing	Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.

Editing Commands Through Keystrokes

The keystrokes help you to edit the command lines. These keystrokes are optional.



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

Table 4: Editing Commands

Editing Commands	Description

Ctrl-B or use the left arrow key	Moves the cursor back one character.
Ctrl-F or use the right arrow key	Moves the cursor forward one character.
Ctrl-A	Moves the cursor to the beginning of the command line.
Ctrl-E	Moves the cursor to the end of the command line.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.
Delete or Backspace key	Erases the character to the left of the cursor.
Ctrl-D	Deletes the character at the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-U or Ctrl-X	Deletes all characters from the cursor to the beginning of the command line.
Ctrl-W	Deletes the word to the left of the cursor.
Esc D	Deletes from the cursor to the end of the word.
Esc C	Capitalizes at the cursor.
Esc L	Changes the word at the cursor to lowercase.
Esc U	Capitalizes letters from the cursor to the end of the word.
Ctrl-V or Esc Q	Designates a particular keystroke as an executable command, perhaps as a shortcut.
Return key	<p>Scrolls down a line or screen on displays that are longer than the terminal screen can display.</p> <p>Note The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including show command output. You can use the Return and Space bar keystrokes whenever you see the More prompt.</p>
Space bar	Scrolls down one screen.

Ctrl-L or **Ctrl-R**

Redisplays the current command line if the controller suddenly sends a message to your screen.

Editing Command Lines That Wrap

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

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

**Note**

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

The following example shows how to wrap a command line that extends beyond a single line on the screen.

SUMMARY STEPS

1. **access-list**
2. **Ctrl-A**
3. **Return** key

DETAILED STEPS

	Command or Action	Purpose
Step 1	access-list Example: <pre>SwitchController(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 SwitchController(config)# \$ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25 SwitchController(config)# \$t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq SwitchController(config)# \$15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45</pre>	Displays the global configuration command entry that extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign (\$) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.
Step 2	Ctrl-A Example: <pre>SwitchController(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0</pre>	Checks the complete syntax. The dollar sign (\$) appears at the end of the line to show that the line has been scrolled to the right.

	Command or Action	Purpose
	10.15.2\$	
Step 3	Return key	Execute the commands. The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the terminal width privileged EXEC command to set the width of your terminal. Use line wrapping with the command history feature to recall and modify previous complex command entries.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

SUMMARY STEPS

1. `{show | more} command | {begin | include | exclude} regular-expression`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>{show more} command {begin include exclude} regular-expression</code> Example: SwitchController# <code>show interfaces include protocol</code> Vlan1 is up, line protocol is up Vlan10 is up, line protocol is down GigabitEthernet1/0/1 is up, line protocol is down GigabitEthernet1/0/2 is up, line protocol is up	Searches and filters the output. Expressions are case sensitive. For example, if you enter <code> exclude output</code> , the lines that contain output are not displayed, but the lines that contain output appear.

Accessing the CLI Through a Console Connection or Through Telnet

Before you can access the CLI, you must connect a terminal or a PC to the controller console or connect a PC to the Ethernet management port and then power on the controller, as described in the hardware installation guide that shipped with your controller.

If your controller is already configured, you can access the CLI through a local console connection or through a remote Telnet session, but your controller must first be configured for this type of access.

You can use one of these methods to establish a connection with the controller:

- Connect the controller console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the controller hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The controller must have network connectivity with the Telnet or SSH client, and the controller must have an enable secret password configured.
 - The controller supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
 - The controller supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.



Using the Web Graphical User Interface

- [Prerequisites for Using the Web GUI, page 13](#)
- [Information About Using The Web GUI, page 13](#)
- [Connecting the Console Port of the Controller , page 15](#)
- [Logging On to the Web GUI, page 15](#)
- [Enabling Web and Secure Web Modes , page 15](#)
- [Configuring the Controller Web GUI, page 16](#)

Prerequisites for Using the Web GUI

- The GUI must be used on a PC running Windows 7, Windows Vista, Windows XP, Windows 2003, or Windows 2000.
- The controller GUI is compatible with Microsoft Internet Explorer 6.0 and 7.0, and Mozilla Firefox up to version 26.0.

Information About Using The Web GUI

A web browser, or graphical user interface (GUI), is built into each controller.

You can use either the service port interface or the management interface to access the GUI. We recommend that you use the service-port interface. Click Help at the top of any page in the GUI to display online help.

You might need to disable your browser's pop-up blocker to view the online help.

Web GUI Features

The controller web GUI supports the following:

The Configuration Wizard—After initial configuration of the IP address and the local username/password or auth via the authentication server (privilege 15 needed), the wizard provides a method to complete the initial

wireless configuration. Start the wizard through Configuration -> Wizard and follow the nine-step process to configure the following:

- Admin Users
- SNMP System Summary
- Management Port
- Wireless Management
- RF Mobility and Country code
- Mobility configuration
- WLANs
- 802.11 Configuration
- Set Time

The Monitor tab:

- Displays summary details of controller, clients, and access points.
- Displays all radio and AP join statistics.
- Displays air quality on access points.
- Displays list of all Cisco Discovery Protocol (CDP) neighbors on all interfaces and the CDP traffic information.
- Displays all rogue access points based on their classification-friendly, malicious, ad hoc, classified, and unclassified.

The Configuration tab:

- Enables you to configure the controller for all initial operation using the web Configuration Wizard. The wizard allows you to configure user details, management interface, and so on.
- Enables you to configure the system, internal DHCP server, management, and mobility management parameters.
- Enables you to configure the controller, WLAN, and radios.
- Enables you to configure and set security policies on your controller.
- Enables you to access the controller operating system software management commands.

The Administration tab enables you to configure system logs.

Connecting the Console Port of the Controller

Before You Begin

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

-
- Step 1** Connect one end of a null-modem serial cable to the controller's RJ-45 console port and the other end to your PC's serial port.
- Step 2** Plug the AC power cord into the controller and a grounded 100 to 240 VAC, 50/60-Hz electrical outlet. Turn on the power supply. The bootup script displays operating system software initialization (code download and power-on self-test verification) and basic configuration. If the controller passes the power-on self-test, the bootup script runs the configuration wizard, which prompts you for basic configuration input.
- Step 3** Enter **yes**. Proceed with basic initial setup configuration parameters in the CLI setup wizard. Specify the IP address for the service port which is the gigabitethernet 0/0 interface.
After entering the configuration parameters in the configuration wizard, you can access the Web GUI. Now, the controller is configured with the IP address for service port.
-

Logging On to the Web GUI

-
- Step 1** Enter the controller IP address in your browser's address bar. For a secure connection, enter `https://ip-address`. For a less secure connection, enter `http://ip-address`.
- Step 2** When prompted, enter a valid username and password and click **OK**.
- Note** The administrative username and password that you created in the configuration wizard are case sensitive. The default username is admin, and the default password is cisco.
The Accessing page appears.
-

Enabling Web and Secure Web Modes

-
- Step 1** Choose **Configuration > Controller > Management > Protocol Management > HTTP-HTTPS**.
The **HTTP-HTTPS Configuration** page appears.
- Step 2** To enable web mode, which allows users to access the controller GUI using "http://ip-address," choose Enabled from the HTTP Access drop-down list. Otherwise, choose Disabled. Web mode (HTTP) is not a secure connection.

- Step 3** To enable secure web mode, which allows users to access the controller GUI using “https://ip-address,” choose Enabled from the HTTPS Access drop-down list. Otherwise, choose Disabled. Secure web mode (HTTPS) is a secure connection.
- Step 4** Choose to track the device in the IP Device Tracking check box.
- Step 5** Choose to enable the trust point in the Enable check box.
- Step 6** Choose the trustpoints from the Trustpoints drop-down list.
- Step 7** Enter the amount of time, in seconds, before the web session times out due to inactivity in the HTTP Timeout-policy (1 to 600 sec) text box.
The valid range is from 1 to 600 seconds.
- Step 8** Enter the server life time in the Server Life Time (1 to 86400 sec) text box.
The valid range is from 1 to 86400 seconds.
- Step 9** Enter the maximum number of connection requests that the server can accept in the Maximum number of Requests (1 to 86400) text box.
The valid range is from 1 to 86400 connections.
- Step 10** Click **Apply**.
- Step 11** Click **Save Configuration**.
-

Configuring the Controller Web GUI

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

-
- Step 1** Connect your PC to the service port and configure an IPv4 address to use the same subnet as the controller. The controller is loaded with IOS XE image and the service port interface is configured as gigabitethernet 0/0.
- Step 2** Start Internet Explorer 10 (or later), Firefox 2.0.0.11 (or later), or Google Chrome on your PC and enter the management interface IP address on the browser window. The management interface IP address is same as the gigabitethernet 0/0 (also known as service port interface). When you log in for the first time, you need to enter HTTP username and password. By default, the username is **admin** and the password is **cisco**.
You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled.
When you log in for the first time, the **Accessing Cisco Controller <Model Number> <Hostname>** page appears.
- Step 3** On the **Accessing Cisco Controller** page, click the **Wireless Web GUI** link to access controller web GUI **Home** page.
- Step 4** Choose **Configuration > Wizard** to perform all steps that you need to configure the controller initially.
The **Admin Users** page appears.
- Step 5** On the **Admin Users** page, enter the administrative username to be assigned to this controller in the User Name text box and the administrative password to be assigned to this controller in the Password and Confirm Password text boxes.
Click **Next**.
The default username is **admin** and the default password is **cisco**. You can also create a new administrator user for the controller. You can enter up to 24 ASCII characters for username and password.

The **SNMP System Summary** page appears.

Step 6 On the **SNMP System Summary** page, enter the following SNMP system parameters for the controller, and click **Next**:

- Customer-definable controller location in the Location text box.
- Customer-definable contact details such as phone number with names in the Contact text box.
- Choose **enabled** to send SNMP notifications for various SNMP traps or **disabled** not to send SNMP notifications for various SNMP traps from the SNMP Global Trap drop-down list.
- Choose **enabled** to send system log messages or **disabled** not to send system log messages from the SNMP Logging drop-down list.

Note The SNMP trap server, must be reachable through the distribution ports (and not through the gigabitethernet0/0 service or management interface).

The **Management Port** page appears.

Step 7 In the **Management Port** page, enter the following parameters for the management port interface (gigabitethernet 0/0) and click **Next**.

- Interface IP address that you assigned for the service port in the IP Address text box.
- Network mask address of the management port interface in the Netmask text box.
- The IPv4 Dynamic Host Configuration Protocol (DHCP) address for the selected port in the IPv4 DHCP Server text box.

The **Wireless Management** page appears.

Step 8 In the **Wireless Management** page, enter the following wireless interface management details, and click **Next**.

- Choose the interface—VLAN, or Ten Gigabit Ethernet from the Select Interface drop-down list.
- VLAN tag identifier, or 0 for no VLAN tag in the VLAN id text box.
- IP address of wireless management interface where access points are connected in the IP Address text box.
- Network mask address of the wireless management interface in the Netmask text box.
- DHCP IPv4 IP address in the IPv4 DHCP Server text box.

When selecting VLAN as interface, you can specify the ports as –Trunk or Access ports from the selected list displayed in the Switch Port Configuration text box.

The **RF Mobility and Country Code** page appears.

Step 9 In the **RF Mobility and Country Code** page, enter the RF mobility domain name in the RF Mobility text box, choose current country code from the Country Code drop-down list, and click **Next**. From the GUI, you can select only one country code.

Note Before configuring RF grouping parameters and mobility configuration, ensure that you refer to the relevant conceptual content and then proceed with the configuration.

The **Mobility Configuration** page with mobility global configuration settings appears.

Step 10 In the **Mobility Configuration** page, view and enter the following mobility global configuration settings, and click **Next**.

- Displays Mobility Controller in the Mobility Role text box.

- Displays mobility protocol port number in the Mobility Protocol Port text box.
 - Displays the mobility group name in the Mobility Group Name text box.
 - Displays whether DTLS is enabled in the DTLS Mode text box.
- DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS.
- Displays mobility domain identifier for 802.11 radios in the Mobility Domain ID for 802.11 radios text box.
 - Displays the number of members configured on the controller in the Mobility Domain Member Count text box.
 - To enable the controller as a Mobility Oracle, select the Mobility Oracle Enabled check box.

Note Only the controller can be configured as Mobility Oracle. You cannot configure the switch as Mobility Oracle.

The Mobility Oracle is optional, it maintains the client database under one complete mobility domain.

- The amount of time (in seconds) between each ping request sent to an peer controller in the Mobility Keepalive Interval (1-30)sec text box.
Valid range is from 1 to 30 seconds, and the default value is 10 seconds.
- Number of times a ping request is sent to an peer controller before the peer is considered to be unreachable in the Mobility Keepalive Count (3-20) text box.
The valid range is from 3 to 20, and the default value is 3.
- The DSCP value that you can set for the mobility controller in the Mobility Control Message DSCP Value (0-63) text box.
The valid range is 0 to 63, and the default value is 0.

The **WLANs** page appears.

Step 11 In the **WLANs** page, enter the following WLAN configuration parameters, and click **Next**.

- WLAN identifier in the WLAN ID text box.
- SSID of the WLAN that the client is associated with in the SSID text box.
- Name of the WLAN used by the client in the Profile Name text box.

The **802.11 Configuration** page appears.

Step 12 In the **802.11 Configuration** page, check either one or both 802.11a/n/ac and 802.11b/g/n check boxes to enable the 802.11 radios, and click **Next**.

The **Set Time** page appears.

Step 13 In the **Set Time** page, you can configure the time and date on the controller based on the following parameters, and click **Next**.

- Displays current timestamp on the controller in the Current Time text box.
- Choose either Manual or NTP from the Mode drop-down list.
On using the NTP server, all access points connected to the controller, synchronizes its time based on the NTP server settings available.
- Choose date on the controller from the Year, Month, and Day drop-down list.

- Choose time from the Hours, Minutes, and Seconds drop-down list.
- Enter the time zone in the Zone text box and select the off setting required when compared to the current time configured on the controller from the Offset drop-down list.

The **Save Wizard** page appears.

- Step 14** In the **Save Wizard** page, you can review the configuration settings performed on the controller using these steps, and if you wish to change any configuration value, click **Previous** and navigate to that page. You can save the controller configuration created using the wizard only if a success message is displayed for all the wizards. If the **Save Wizard** page displays errors, you must recreate the wizard for initial configuration of the controller.
-



Preventing Unauthorized Access

- [Finding Feature Information, page 21](#)
- [Preventing Unauthorized Access, page 21](#)

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 34](#)

[TACACS+ and Switch Access, on page 45](#)

[Setting a Telnet Password for a Terminal Line, on page 32](#)



CHAPTER

4

Controlling Switch Access with Passwords and Privilege Levels

- [Finding Feature Information, page 23](#)
- [Restrictions for Controlling Switch Access with Passwords and Privileges, page 23](#)
- [Information About Passwords and Privilege Levels, page 24](#)
- [How to Control Switch Access with Passwords and Privilege Levels, page 26](#)
- [Monitoring Switch Access, page 40](#)
- [Configuration Examples for Setting Passwords and Privilege Levels, page 40](#)
- [Additional References, page 41](#)

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 30](#)

[Password Recovery, on page 25](#)

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 5: Default Password and Privilege Levels

Feature	Default Setting
Enable password and privilege level	No password is defined. The default is level 15 (privileged EXEC level). The password is not encrypted in the configuration file.
Enable secret password and privilege level	No password is defined. The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
Line password	No password is defined.

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 28](#)

[Example: Protecting Enable and Enable Secret Passwords with Encryption, on page 41](#)

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 30](#)

[Restrictions for Controlling Switch Access with Passwords and Privileges, on page 23](#)

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 32](#)

[Example: Setting a Telnet Password for a Terminal Line, on page 41](#)

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 34](#)

Privilege Levels

Cisco switches (and other 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 36](#)

[Example: Setting the Privilege Level for a Command, on page 41](#)

[Changing the Default Privilege Level for Lines, on page 38](#)

[Logging into and Exiting a Privilege Level, on page 39](#)

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **enable password** *password*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	enable password <i>password</i> Example: SwitchController(config)# enable password secret321	<p>Defines a new password or changes an existing password for access to privileged EXEC mode.</p> <p>By default, no password is defined.</p> <p>For <i>password</i>, 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 Crtl-v when you create the password; for example, to create the password abc?123, do this:</p> <ol style="list-style-type: none"> 1 Enter abc. 2 Enter Crtl-v. 3 Enter ?123. <p>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.</p>

	Command or Action	Purpose
Step 4	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.
Step 5	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 6	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Related Topics

[Example: Setting or Changing a Static Enable Password, on page 40](#)

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Use one of the following:
 - **enable password** [*level level*]
 {*password* | *encryption-type encrypted-password*}
 - **enable secret** [*level level*]
 {*password* | *encryption-type encrypted-password*}
4. **service password-encryption**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	Use one of the following: <ul style="list-style-type: none"> • enable password [<i>level level</i>] {<i>password</i> <i>encryption-type encrypted-password</i>} • enable secret [<i>level level</i>] {<i>password</i> <i>encryption-type encrypted-password</i>} Example: SwitchController(config)# enable password example102	<ul style="list-style-type: none"> • Defines a new password or changes an existing password for access to privileged EXEC mode. • Defines a secret password, which is saved using a nonreversible encryption method. <ul style="list-style-type: none"> ◦ (Optional) For <i>level</i>, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges). ◦ For <i>password</i>, 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. ◦ (Optional) For <i>encryption-type</i>, only type 5, a Cisco proprietary encryption algorithm, is available. If you

	Command or Action	Purpose
	or <pre>SwitchController(config)# enable secret level 1 password secret123sample</pre>	specify an encryption type, you must provide an encrypted password—an encrypted password that you copy from another switch configuration. Note If you specify an encryption type and then enter a clear text password, you can not re-enter privileged EXEC mode. You cannot recover a lost encrypted password by any method.
Step 4	service password-encryption Example: <pre>SwitchController(config)# service password-encryption</pre>	(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.
Step 5	end Example: <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 6	show running-config Example: <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 7	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

[Additional Password Security, on page 24](#)

[Example: Protecting Enable and Enable Secret Passwords with Encryption, on page 41](#)

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no service password-recovery**
4. **end**
5. **show version**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	no service password-recovery Example: SwitchController (config) # no service password-recovery	Disables password recovery. This setting is saved in an area of the flash memory that is accessible by the boot loader and the Cisco IOS image, but it is not part of the file system and is not accessible by any user.
Step 4	end Example: SwitchController (config) # end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	show version Example: SwitchController# show version	Verifies the configuration by checking the last few lines of the command output.
Step 6	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 7	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

What to Do Next

To re-enable password recovery, use the **service password-recovery** global configuration command.

Related Topics

[Password Recovery, on page 25](#)

[Restrictions for Controlling Switch Access with Passwords and Privileges, on page 23](#)

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line vty 0 15**
4. **password *password***
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Note If a password is required for access to privileged EXEC mode, you will be prompted for it. Enters privileged EXEC mode.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	line vty 0 15 Example: SwitchController(config)# line vty 0 15	Configures the number of Telnet sessions (lines), and enters line configuration mode. There are 16 possible sessions on a command-capable SwitchController. The 0 and 15 mean that you are configuring all 16 possible Telnet sessions.
Step 4	password <i>password</i> Example: SwitchController(config-line)# password abcxyz543	Sets a Telnet password for the line or lines. For <i>password</i> , 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.
Step 5	end Example: SwitchController(config-line)# end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 7	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Related Topics

[Information about Passwords and Privilege Levels](#)

[Preventing Unauthorized Access, on page 21](#)

[Terminal Line Telnet Configuration, on page 25](#)

[Example: Setting a Telnet Password for a Terminal Line, on page 41](#)

Configuring Username and Password Pairs

Follow these steps to configure username and password pairs:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **username** *name* [**privilege** *level*] {**password** *encryption-type password*}
4. Use one of the following:
 - **line console 0**
 - **line vty 0 15**
5. **login local**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>SwitchController> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p>username <i>name</i> [privilege <i>level</i>] {password <i>encryption-type password</i>}</p> <p>Example:</p> <pre>SwitchController(config)# username adamsample privilege 1 password secret456</pre> <pre>SwitchController(config)# username 111111111111 mac attribute</pre>	<p>Sets the username, privilege level, and password for each user.</p> <ul style="list-style-type: none"> • For <i>name</i>, specify the user ID as one word or the MAC address. Spaces and quotation marks are not allowed. • You can configure a maximum of 12000 clients each, for both username and MAC filter. • (Optional) For <i>level</i>, 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. • For <i>encryption-type</i>, enter 0 to specify that an unencrypted password will follow. Enter 7 to specify that a hidden password will follow. • For <i>password</i>, specify the password the user must enter to gain access to the SwitchController. 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 4	<p>Use one of the following:</p> <ul style="list-style-type: none"> • line console 0 • line vty 0 15 <p>Example:</p> <pre>SwitchController(config)# line console 0</pre> <p>or</p> <pre>SwitchController(config)# line vty 15</pre>	Enters line configuration mode, and configures the console port (line 0) or the VTY lines (line 0 to 15).

	Command or Action	Purpose
Step 5	login local Example: SwitchController(config-line)# login local	Enables local password checking at login time. Authentication is based on the username specified in Step 3.
Step 6	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.
Step 7	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 8	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Related Topics

[Information about Passwords and Privilege Levels](#)

[Preventing Unauthorized Access, on page 21](#)

[Username and Password Pairs, on page 25](#)

Setting the Privilege Level for a Command

Follow these steps to set the privilege level for a command:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **privilege mode level level command**
4. **enable password level level password**
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>SwitchController> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p>privilege mode level level command</p> <p>Example:</p> <pre>SwitchController(config)# privilege exec level 14 configure</pre>	<p>Sets the privilege level for a command.</p> <ul style="list-style-type: none"> For <i>mode</i>, enter configure for global configuration mode, exec for EXEC mode, interface for interface configuration mode, or line for line configuration mode. For <i>level</i>, 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. For <i>command</i>, specify the command to which you want to restrict access.
Step 4	<p>enable password level level password</p> <p>Example:</p> <pre>SwitchController(config)# enable password level 14 SecretPswd14</pre>	<p>Specifies the password to enable the privilege level.</p> <ul style="list-style-type: none"> For <i>level</i>, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. For <i>password</i>, 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.
Step 5	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 6	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics[Privilege Levels, on page 26](#)[Example: Setting the Privilege Level for a Command, on page 41](#)

Changing the Default Privilege Level for Lines

Follow these steps to change the default privilege level for the specified line:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line vty *line***
4. **privilege level *level***
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	line vty <i>line</i> Example: SwitchController(config)# line vty 10	Selects the virtual terminal line on which to restrict access.
Step 4	privilege level <i>level</i> Example: SwitchController(config)# privilege level 15	Changes the default privilege level for the line. For <i>level</i> , 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.

	Command or Action	Purpose
Step 5	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

What to Do Next

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.

Related Topics

[Privilege Levels, on page 26](#)

Logging into and Exiting a Privilege Level

Beginning in user EXEC mode, follow these steps to log into a specified privilege level and exit a specified privilege level.

SUMMARY STEPS

1. **enable level**
2. **disable level**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable level	Logs in to a specified privilege level.

	Command or Action	Purpose
	Example: SwitchController> enable 15	Following the example, Level 15 is privileged EXEC mode. For <i>level</i> , the range is 0 to 15.
Step 2	disable level Example: SwitchController# disable 1	Exits to a specified privilege level. Following the example, Level 1 is user EXEC mode. For <i>level</i> , the range is 0 to 15.

Related Topics

[Privilege Levels, on page 26](#)

Monitoring Switch Access

Table 6: Commands for Displaying DHCP Information

show privilege	Displays the privilege level configuration.
-----------------------	---

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 *11u2c3k4y5*. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
SwitchController(config)# enable password 11u2c3k4y5
```

Related Topics

[Setting or Changing a Static Enable Password, on page 26](#)

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:

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

Related Topics

[Protecting Enable and Enable Secret Passwords with Encryption](#), on page 28

[Additional Password Security](#), on page 24

Example: Setting a Telnet Password for a Terminal Line

This example shows how to set the Telnet password to *let45me67in89*:

```
SwitchController(config)# line vty 10
SwitchController(config-line)# password let45me67in89
```

Related Topics

[Setting a Telnet Password for a Terminal Line](#), on page 32

[Terminal Line Telnet Configuration](#), on page 25

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:

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

Related Topics

[Setting the Privilege Level for a Command](#), on page 36

[Privilege Levels](#), on page 26

Additional References

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

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/support</p>



Configuring TACACS+

- [Finding Feature Information, page 43](#)
- [Prerequisites for Controlling Switch Access with Terminal Access Controller Access Control System Plus \(TACACS+\), page 43](#)
- [Information About TACACS+, page 45](#)
- [How to Configure TACACS+, page 49](#)
- [Monitoring TACACS+, page 58](#)
- [Additional References, page 58](#)

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 Terminal Access Controller Access Control System Plus (TACACS+)

The following are the prerequisites for set up and configuration of switch access with Terminal Access Controller Access Control System Plus (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 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 45

[TACACS+ Operation](#), on page 47

[How to Configure TACACS+](#), on page 49

[Method List](#), on page 48

[Configuring TACACS+ Login Authentication](#), on page 51

[TACACS+ Login Authentication](#), on page 48

[Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services](#), on page 54

[TACACS+ Authorization for Privileged EXEC Access and Network Services](#), on page 48

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

[Information about Passwords and Privilege Levels](#)

[Preventing Unauthorized Access, on page 21](#)

[Configuring the Switch for Local Authentication and Authorization, on page 107](#)

[SSH Servers, Integrated Clients, and Supported Versions, on page 133](#)

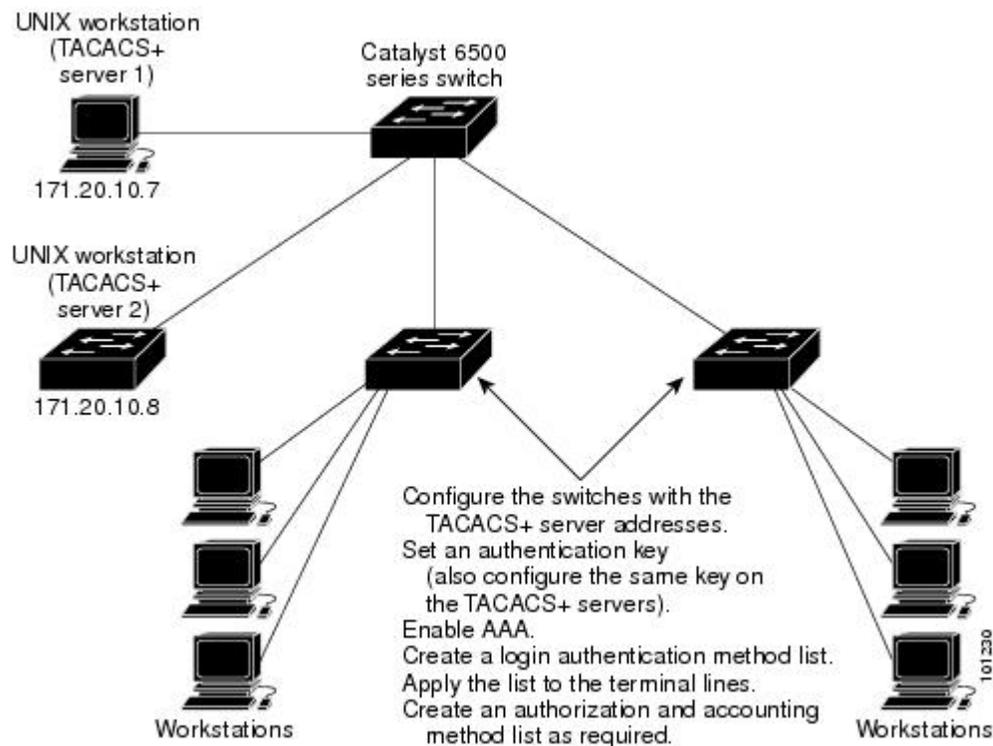
TACACS+ Overview

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—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

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 1: 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 Controlling Switch Access with Terminal Access Controller Access Control System Plus \(TACACS+\), on page 43](#)

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 Controlling Switch Access with Terminal Access Controller Access Control System Plus \(TACACS+\), on page 43](#)

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 TACACS+, on page 49](#)

[Prerequisites for Controlling Switch Access with Terminal Access Controller Access Control System Plus \(TACACS+\), on page 43](#)

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 49](#)

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.

Related Topics

[Configuring TACACS+ Login Authentication, on page 51](#)

[Prerequisites for Controlling Switch Access with Terminal Access Controller Access Control System Plus \(TACACS+\), on page 43](#)

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.

Related Topics

[Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services](#), on page 54
[Prerequisites for Controlling Switch Access with Terminal Access Controller Access Control System Plus \(TACACS+\)](#), on page 43

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.

Related Topics

[Starting TACACS+ Accounting](#), on page 56

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 TACACS+

This section describes how to configure your switch to support TACACS+.

Related Topics

[Method List](#), on page 48

[Prerequisites for Controlling Switch Access with Terminal Access Controller Access Control System Plus \(TACACS+\)](#), on page 43

Identifying the TACACS+ Server Host and Setting the Authentication Key

Follow these steps to identify the TACACS+ server host and set the authentication key:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tacacs-server host *hostname***
4. **aaa new-model**
5. **aaa group server tacacs+ *group-name***
6. **server *ip-address***
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	tacacs-server host <i>hostname</i> Example: SwitchController(config)# tacacs-server host 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 <i>hostname</i> , specify the name or IP address of the host.
Step 4	aaa new-model Example: SwitchController(config)# aaa new-model	Enables AAA.
Step 5	aaa group server tacacs+ <i>group-name</i> Example: SwitchController(config)# aaa group server tacacs+ your_server_group	(Optional) Defines the AAA server-group with a group name. This command puts the SwitchController in a server group subconfiguration mode.

	Command or Action	Purpose
Step 6	<p><code>server ip-address</code></p> <p>Example:</p> <pre>SwitchController(config)# server 10.1.2.3</pre>	<p>(Optional) Associates a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group.</p> <p>Each server in the group must be previously defined in Step 3.</p>
Step 7	<p><code>end</code></p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 8	<p><code>show running-config</code></p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 9	<p><code>copy running-config startup-config</code></p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

[TACACS+ Configuration Options, on page 48](#)

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 controller for HTTP access by using AAA methods, you must configure the controller with the `ip http authentication aaa` global configuration command. Configuring AAA authentication does not secure the controller 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*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {default | list-name} method1 [method2...]
5. **line** [console | tty | vty] line-number [ending-line-number]
6. **login authentication** {default | list-name}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	aaa new-model Example: SwitchController(config)# aaa new-model	Enables AAA.
Step 4	aaa authentication login {default list-name} method1 [method2...] Example: SwitchController(config)# aaa authentication login default tacacs+ local	Creates a login authentication method list. <ul style="list-style-type: none"> • To create a default list that is used when a named list is <i>not</i> 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 <i>list-name</i>, specify a character string to name the list you are creating. • For <i>method1...</i>, 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:

	Command or Action	Purpose
		<ul style="list-style-type: none"> • <i>enable</i>—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. • <i>group tacacs+</i>—Uses TACACS+ authentication. Before you can use this authentication method, you must configure the TACACS+ server. For more information, see the Identifying the TACACS+ Server Host and Setting the Authentication Key, on page 49. • <i>line</i> —Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the password password line configuration command. • <i>local</i>—Use the local username database for authentication. You must enter username information in the database. Use the username password global configuration command. • <i>local-case</i>—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the username name password global configuration command. • <i>none</i>—Do not use any authentication for login.
Step 5	line [console tty vtty] <i>line-number</i> [<i>ending-line-number</i>] Example: SwitchController(config)# line 2 4	Enters line configuration mode, and configures the lines to which you want to apply the authentication list.
Step 6	login authentication { default <i>list-name</i> } Example: SwitchController(config-line)# login authentication default	Applies the authentication list to a line or set of lines. <ul style="list-style-type: none"> • If you specify default, use the default list created with the aaa authentication login command. • For <i>list-name</i>, specify the list created with the aaa authentication login command.
Step 7	end Example: SwitchController(config-line)# end	Returns to privileged EXEC mode.
Step 8	show running-config Example: SwitchController# show running-config	Verifies your entries.

	Command or Action	Purpose
Step 9	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

[TACACS+ Login Authentication](#), on page 48

[Prerequisites for Controlling Switch Access with Terminal Access Controller Access Control System Plus \(TACACS+\)](#), on page 43

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization network tacacs+**
4. **aaa authorization exec tacacs+**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>SwitchController> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p>aaa authorization network tacacs+</p> <p>Example:</p> <pre>SwitchController(config)# aaa authorization network tacacs+</pre>	Configures the switch for user TACACS+ authorization for all network-related service requests.
Step 4	<p>aaa authorization exec tacacs+</p> <p>Example:</p> <pre>SwitchController(config)# aaa authorization exec tacacs+</pre>	<p>Configures the switch for user TACACS+ authorization if the user has privileged EXEC access.</p> <p>The exec keyword might return user profile information (such as autocommand information).</p>
Step 5	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 6	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 7	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

[TACACS+ Authorization for Privileged EXEC Access and Network Services](#), on page 48

[Prerequisites for Controlling Switch Access with Terminal Access Controller Access Control System Plus \(TACACS+\)](#), on page 43

Starting TACACS+ Accounting

Follow these steps to start TACACS+ Accounting:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting network start-stop tacacs+**
4. **aaa accounting exec start-stop tacacs+**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	aaa accounting network start-stop tacacs+ Example: SwitchController(config)# aaa accounting network start-stop tacacs+	Enables TACACS+ accounting for all network-related service requests.
Step 4	aaa accounting exec start-stop tacacs+ Example: SwitchController(config)# aaa accounting exec	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.

	Command or Action	Purpose
	<code>start-stop tacacs+</code>	
Step 5	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.
Step 6	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 7	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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 49](#)

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 7: Commands for Displaying TACACS+ Information

Command	Purpose
show tacacs	Displays TACACS+ server statistics.

Additional References

Related Documents

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.html
Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850-library.html

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

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support



Configuring RADIUS

- [Finding Feature Information, page 61](#)
- [Prerequisites for Controlling SwitchController Access with RADIUS, page 61](#)
- [Restrictions for Controlling SwitchController Access with RADIUS, page 62](#)
- [Information about RADIUS, page 63](#)
- [How to Configure RADIUS, page 74](#)
- [Monitoring CoA Functionality, page 93](#)
- [Configuration Examples for Controlling Switch Access with RADIUS, page 94](#)
- [Additional References, page 96](#)

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 SwitchController Access with RADIUS

This section lists the prerequisites for controlling SwitchController access with RADIUS.

General:

- RADIUS and 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.

- 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 SwitchController.
- 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 63

[RADIUS Operation](#), on page 64

Restrictions for Controlling SwitchController Access with RADIUS

This topic covers restrictions for controlling SwitchController 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 63

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 Controlling SwitchController Access with RADIUS](#), on page 61

[Configuring the Switch for Local Authentication and Authorization](#), on page 107

[SSH Servers, Integrated Clients, and Supported Versions](#), on page 133

RADIUS Overview

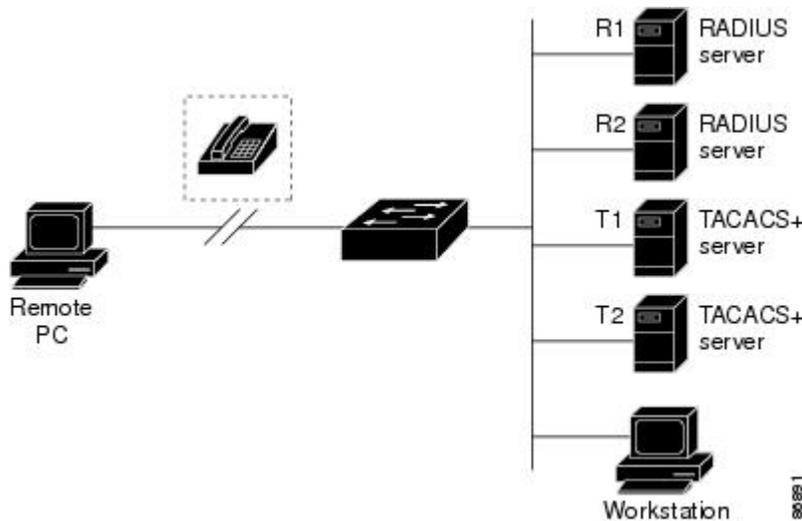
RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco routers and switches. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

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 SwitchController 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.

Figure 2: Transitioning from RADIUS to TACACS+ Services



Related Topics

[Restrictions for Controlling SwitchController Access with RADIUS, on page 62](#)

RADIUS Operation

When a user attempts to log in and authenticate to a SwitchController 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 Controlling SwitchController Access with RADIUS](#), on page 61

RADIUS Change of Authorization

This section provides an overview of the RADIUS interface including available primitives and how they are used during a Change of Authorization (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 controllers support the RADIUS Change of Authorization (CoA) extensions defined in RFC 5176 that are typically used in a pushed model and allow for the dynamic reconfiguring of sessions from external authentication, authorization, and accounting (AAA) or policy servers.

The controller 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 Identity Services Engine, and Cisco Secure Access Control Server (ACS) 5.1.

The RADIUS interface is enabled by default on Catalyst controllers. 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.

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 8: Supported IETF Attributes

Attribute Number	Attribute Name
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

This table shows the possible values for the Error-Cause attribute.

Table 9: Error-Cause Values

Value	Explanation
201	Residual Session Context Removed
202	Invalid EAP Packet (Ignored)
401	Unsupported Attribute
402	Missing Attribute
403	NAS Identification Mismatch
404	Invalid Request
405	Unsupported Service
406	Unsupported Extension
407	Invalid Attribute Value
501	Administratively Prohibited

Value	Explanation
502	Request Not Routable (Proxy)
503	Session Context Not Found
504	Session Context Not Removable
505	Other Proxy Processing Error
506	Resources Unavailable
507	Request Initiated
508	Multiple Session Selection Unsupported

CoA Request Response Code

The CoA Request response code can be used to convey a command to the switch.

Related Topics

[CoA Request Commands, on page 68](#)

Session Identification

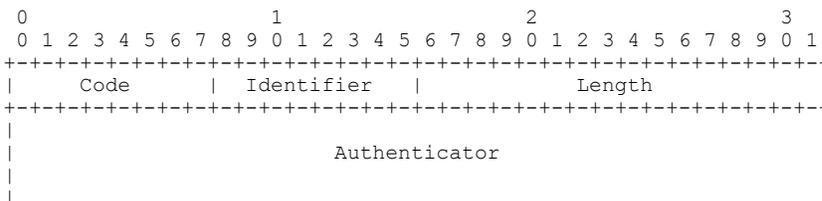
For disconnect and CoA requests targeted at a particular session, the switch locates the session based on one or more of the following attributes:

- Calling-Station-Id (IETF attribute #31 which contains the host MAC address)
- Audit-Session-Id (Cisco VSA)
- Acct-Session-Id (IETF attribute #44)

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.



```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Attributes ...
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

The attributes field is used to carry Cisco vendor-specific attributes (VSAs).

Related Topics

- [CoA Disconnect-Request, on page 69](#)
- [CoA Request: Disable Host Port, on page 70](#)
- [CoA Request: Bounce-Port, on page 70](#)

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 10: CoA Commands Supported on the controller

Command ¹	Cisco VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	This is a standard disconnect request that does not require a VSA.
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

¹ All CoA commands must include the session identifier between the controller and the CoA client.

Related Topics

- [CoA Request Response Code, on page 67](#)

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's 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. 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 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 67](#)

CoA Request: Disable Host Port

This command is carried in a standard CoA-Request message that has this new 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. 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 67](#)

CoA Request: Bounce-Port

This command 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 67](#)

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 74](#)

[Defining AAA Server Groups, on page 79](#)

[Configuring Settings for All RADIUS Servers, on page 86](#)

[Configuring RADIUS Login Authentication, on page 77](#)

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 77](#)

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. 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.

Related Topics

[Defining AAA Server Groups, on page 79](#)

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 82](#)

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 84](#)

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 attributevalue (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.

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)."

For a complete list of RADIUS attributes or more information about vendor-specific attribute 26, see the "RADIUS Attributes" appendix in the *Cisco IOS Security Configuration Guide*.

Related Topics

[Configuring the Controller to Use Vendor-Specific RADIUS Attributes, on page 87](#)

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 Controller for Vendor-Proprietary RADIUS Server Communication, on page 89](#)

How to Configure RADIUS

Identifying the RADIUS Server Host

To apply these settings globally to all RADIUS servers communicating with the SwitchController, use the three unique global configuration commands: **radius-server timeout**, **radius-server retransmit**, and **radius-server key**. To apply these values on a specific RADIUS server, use the **radius-server host** global configuration command.

You can configure the SwitchController 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 SwitchController and the key string to be shared by both the server and the SwitchController. 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 controller, 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	radius-server host { <i>hostname</i> <i>ip-address</i> } [auth-port <i>port-number</i>] [acct-port <i>port-number</i>] [timeout <i>seconds</i>] [retransmit <i>retries</i>] [key <i>string</i>] Example: SwitchController(config)# radius-server host 172.29.36.49	Specifies the IP address or hostname of the remote RADIUS server host. <ul style="list-style-type: none"> • (Optional) For auth-port <i>port-number</i>, specify the UDP destination port for authentication requests. • (Optional) For acct-port <i>port-number</i>, specify the UDP destination port for accounting requests. • (Optional) For timeout <i>seconds</i>, specify the time interval that the SwitchController waits for the RADIUS server to reply before resending.

	Command or Action	Purpose
	<code>auth-port 1612 key rad1</code>	<p>The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used.</p> <ul style="list-style-type: none"> • (Optional) For retransmit <i>retries</i>, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used. • (Optional) For key <i>string</i>, specify the authentication and encryption key used between the SwitchController and the RADIUS daemon running on the RADIUS server. <p>Note The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</p> <p>To configure the SwitchController to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The SwitchController software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.</p>
Step 4	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 6	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

[RADIUS Server Host, on page 72](#)

[Defining AAA Server Groups, on page 79](#)

[Configuring Settings for All RADIUS Servers, on page 86](#)

Configuring RADIUS Login Authentication

Follow these steps to configure RADIUS login authentication:

Before You Begin

To secure the controller for HTTP access by using AAA methods, you must configure the controller with the **ip http authentication aaa** global configuration command. Configuring AAA authentication does not secure the controller for HTTP access by using AAA methods.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login {default | list-name} method1 [method2...]**
5. **line [console | tty | vty] line-number [ending-line-number]**
6. **login authentication {default | list-name}**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	aaa new-model Example: <pre>SwitchController(config)# aaa new-model</pre>	Enables AAA.
Step 4	aaa authentication login {default list-name} method1 [method2...] Example: <pre>SwitchController(config)# aaa authentication login default local</pre>	<p>Creates a login authentication method list.</p> <ul style="list-style-type: none"> • To create a default list that is used when a named list is <i>not</i> 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 <i>list-name</i>, specify a character string to name the list you are creating. • For <i>method1...</i>, 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. <p>Select one of these methods:</p> <ul style="list-style-type: none"> ◦ <i>enable</i>—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. ◦ <i>group radius</i>—Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server. ◦ <i>line</i>—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the password password line configuration command. ◦ <i>local</i>—Use the local username database for authentication. You must enter username information in the database. Use the username name password global configuration command. ◦ <i>local-case</i>—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the username password global configuration command. ◦ <i>none</i>—Do not use any authentication for login.

	Command or Action	Purpose
Step 5	<p>line [console tty vty] <i>line-number</i> [<i>ending-line-number</i>]</p> <p>Example:</p> <pre>SwitchController(config)# line 1 4</pre>	Enters line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 6	<p>login authentication {default <i>list-name</i>}</p> <p>Example:</p> <pre>SwitchController(config)# login authentication default</pre>	<p>Applies the authentication list to a line or set of lines.</p> <ul style="list-style-type: none"> • If you specify default, use the default list created with the aaa authentication login command. • For <i>list-name</i>, specify the list created with the aaa authentication login command.
Step 7	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 8	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 9	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

[RADIUS Login Authentication, on page 72](#)

[RADIUS Server Host, on page 72](#)

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
4. **aaa new-model**
5. **aaa group server radius** *group-name*
6. **server** *ip-address*
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	radius-server host { <i>hostname</i> <i>ip-address</i> } [auth-port <i>port-number</i>] [acct-port <i>port-number</i>] [timeout <i>seconds</i>] [retransmit <i>retries</i>] [key <i>string</i>] Example: SwitchController(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1	Specifies the IP address or hostname of the remote RADIUS server host. <ul style="list-style-type: none"> • (Optional) For auth-port <i>port-number</i>, specify the UDP destination port for authentication requests. • (Optional) For acct-port <i>port-number</i>, specify the UDP destination port for accounting requests. • (Optional) For timeout <i>seconds</i>, specify the time interval that the controller waits for the RADIUS server to reply before resending. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used. • (Optional) For retransmit <i>retries</i>, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used.

	Command or Action	Purpose
		<ul style="list-style-type: none"> (Optional) For key string, specify the authentication and encryption key used between the controller and the RADIUS daemon running on the RADIUS server. <p>Note The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</p> <p>To configure the controller to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The controller software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.</p>
Step 4	aaa new-model Example: <pre>SwitchController(config)# aaa new-model</pre>	Enables AAA.
Step 5	aaa group server radius group-name Example: <pre>SwitchController(config)# aaa group server radius group1</pre>	Defines the AAA server-group with a group name. This command puts the controller in a server group configuration mode.
Step 6	server ip-address Example: <pre>SwitchController(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001</pre>	Associates a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined in Step 2.
Step 7	end Example: <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 8	show running-config Example: <pre>SwitchController# show running-config</pre>	Verifies your entries.

	Command or Action	Purpose
Step 9	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Related Topics

[Identifying the RADIUS Server Host, on page 74](#)

[RADIUS Server Host, on page 72](#)

[AAA Server Groups, on page 73](#)

Configuring RADIUS Authorization for User Privileged Access and Network Services



Note

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization network radius**
4. **aaa authorization exec radius**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	aaa authorization network radius Example: SwitchController(config)# aaa authorization network radius	Configures the controller for user RADIUS authorization for all network-related service requests.
Step 4	aaa authorization exec radius Example: SwitchController(config)# aaa authorization exec radius	Configures the controller for user RADIUS authorization if the user has privileged EXEC access. The exec keyword might return user profile information (such as autocommand information).
Step 5	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.
Step 6	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 7	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

What to Do Next

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

The **aaa authorization exec radius local** command sets these authorization parameters:

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

Related Topics

[AAA Authorization, on page 73](#)

Starting RADIUS Accounting

Follow these steps to start RADIUS accounting:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting network start-stop radius**
4. **aaa accounting exec start-stop radius**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	aaa accounting network start-stop radius Example: <pre>SwitchController(config)# aaa accounting network start-stop radius</pre>	Enables RADIUS accounting for all network-related service requests.
Step 4	aaa accounting exec start-stop radius Example: <pre>SwitchController(config)# aaa accounting exec start-stop radius</pre>	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: <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 6	show running-config Example: <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 7	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

What to Do Next

To establishing a session with a router if the AAA server is unreachable, use the **aaa accounting system guarantee-first** command. This 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.

Related Topics

[RADIUS Accounting, on page 73](#)

Configuring Settings for All RADIUS Servers

Beginning in privileged EXEC mode, follow these steps to configure settings for all RADIUS servers:

SUMMARY STEPS

1. **configure terminal**
2. **radius-server key *string***
3. **radius-server retransmit *retries***
4. **radius-server timeout *seconds***
5. **radius-server deadtime *minutes***
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	radius-server key <i>string</i> Example: SwitchController(config)# radius-server key <i>your_server_key</i>	Specifies the shared secret text string used between the switch and all RADIUS servers. Note 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.
Step 3	radius-server retransmit <i>retries</i> Example: SwitchController(config)# radius-server retransmit 5	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.
Step 4	radius-server timeout <i>seconds</i> Example: SwitchController(config)# radius-server timeout 3	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.

	Command or Action	Purpose
Step 5	radius-server <i>deadtime</i> <i>minutes</i> Example: <pre>SwitchController(config)# radius-server deadtime 0</pre>	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.
Step 6	end Example: <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.

Related Topics

- [Identifying the RADIUS Server Host, on page 74](#)
- [RADIUS Server Host, on page 72](#)

Configuring the Controller to Use Vendor-Specific RADIUS Attributes

Follow these steps to configure the controller to use vendor-specific RADIUS attributes:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send [accounting | authentication]**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>SwitchController> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p>radius-server vsa send [accounting authentication]</p> <p>Example:</p> <pre>SwitchController(config)# radius-server vsa send</pre>	<p>Enables the controller to recognize and use VSAs as defined by RADIUS IETF attribute 26.</p> <ul style="list-style-type: none"> • (Optional) Use the accounting keyword to limit the set of recognized vendor-specific attributes to only accounting attributes. • (Optional) Use the authentication keyword to limit the set of recognized vendor-specific attributes to only authentication attributes. <p>If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.</p>
Step 4	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 6	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

[Vendor-Specific RADIUS Attributes, on page 74](#)

Configuring the Controller for Vendor-Proprietary RADIUS Server Communication

Follow these steps to configure the controller to use vendor-proprietary RADIUS server communication:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host {hostname | ip-address} non-standard**
4. **radius-server key string**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	radius-server host {hostname ip-address} non-standard Example: SwitchController(config)# radius-server host 172.20.30.15 nonstandard	Specifies the IP address or hostname of the remote RADIUS server host and identifies that it is using a vendor-proprietary implementation of RADIUS.
Step 4	radius-server key string Example: SwitchController(config)# radius-server	Specifies the shared secret text string used between the controller and the vendor-proprietary RADIUS server. The controller and the RADIUS server use this text string to encrypt passwords and exchange responses.

	Command or Action	Purpose
	<code>key rad124</code>	Note 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.
Step 5	<code>end</code> Example: <code>SwitchController(config)# end</code>	Returns to privileged EXEC mode.
Step 6	<code>show running-config</code> Example: <code>SwitchController# show running-config</code>	Verifies your entries.
Step 7	<code>copy running-config startup-config</code> Example: <code>SwitchController# copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

What to Do Next

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*.

Related Topics

[Vendor-Proprietary RADIUS Server Communication, on page 74](#)

Configuring CoA on the Controller

Follow these steps to configure CoA on a controller. This procedure is required.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-address* | *name*} [*vrf vrfname*] [**server-key** *string*]
6. **server-key** [0 | 7] *string*
7. **port** *port-number*
8. **auth-type** {*any* | *all* | *session-key*}
9. **ignore session-key**
10. **ignore server-key**
11. **authentication command bounce-port ignore**
12. **authentication command disable-port ignore**
13. **end**
14. **show running-config**
15. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	aaa new-model Example: SwitchController(config)# aaa new-model	Enables AAA.
Step 4	aaa server radius dynamic-author Example: SwitchController(config)# aaa server radius dynamic-author	Configures the controller as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server.

	Command or Action	Purpose
Step 5	<code>client {ip-address name} [vrf vrfname] [server-key string]</code>	Enters dynamic authorization local server configuration mode and specifies a RADIUS client from which a device will accept CoA and disconnect requests.
Step 6	<code>server-key [0 7] string</code> Example: <pre>SwitchController(config-sg-radius)# server-key your_server_key</pre>	Configures the RADIUS key to be shared between a device and RADIUS clients.
Step 7	<code>port port-number</code> Example: <pre>SwitchController(config-sg-radius)# port 25</pre>	Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients.
Step 8	<code>auth-type {any all session-key}</code> Example: <pre>SwitchController(config-sg-radius)# auth-type any</pre>	Specifies the type of authorization the controller uses for RADIUS clients. The client must match all the configured attributes for authorization.
Step 9	<code>ignore session-key</code>	(Optional) Configures the controller to ignore the session-key. For more information about the ignore command, see the <i>Cisco IOS Intelligent Services Gateway Command Reference</i> on Cisco.com.
Step 10	<code>ignore server-key</code> Example: <pre>SwitchController(config-sg-radius)# ignore server-key</pre>	(Optional) Configures the controller to ignore the server-key. For more information about the ignore command, see the <i>Cisco IOS Intelligent Services Gateway Command Reference</i> on Cisco.com.
Step 11	<code>authentication command bounce-port ignore</code> Example: <pre>SwitchController(config-sg-radius)# authentication command bounce-port ignore</pre>	(Optional) Configures the controller 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.
Step 12	<code>authentication command disable-port ignore</code> Example: <pre>SwitchController(config-sg-radius)# authentication command disable-port ignore</pre>	(Optional) Configures the controller 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.

	Command or Action	Purpose
Step 13	end Example: SwitchController(config-sg-radius)# end	Returns to privileged EXEC mode.
Step 14	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 15	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Monitoring CoA Functionality

Table 11: Privileged EXEC show Commands

Command	Purpose
show aaa attributes protocol radius	Displays AAA attributes of RADIUS commands.

Table 12: Global Troubleshooting Commands

Command	Purpose
debug radius	Displays information for troubleshooting RADIUS.
debug aaa coa	Displays information for troubleshooting CoA processing.
debug aaa pod	Displays information for troubleshooting POD packets.
debug aaa subsys	Displays information for troubleshooting POD packets.

Command	Purpose
<code>debug cmdhd [detail error events]</code>	Displays information for troubleshooting command headers.

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:

```
SwitchController(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
SwitchController(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

This example shows how to configure *host1* as the RADIUS server and to use the default ports for both authentication and accounting:

```
SwitchController(config)# radius-server host host1
```

Example: Using Two Different RADIUS Group Servers

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

```
SwitchController(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
SwitchController(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
SwitchController(config)# aaa new-model
SwitchController(config)# aaa group server radius group1
SwitchController(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
SwitchController(config-sg-radius)# exit
SwitchController(config)# aaa group server radius group2
SwitchController(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
SwitchController(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:

```
cisco-avpair= "tunnel-type (#64)=VLAN (13)"
cisco-avpair= "tunnel-medium-type (#65)=802 media (6)"
cisco-avpair= "tunnel-private-group-id (#81)=vlanid"
```

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:

```
SwitchController(config)# radius-server host 172.20.30.15 nonstandard
SwitchController(config)# radius-server key rad124
```

Additional References

Related Documents

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.html
Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850-library.html

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

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/support</p>



Configuring Kerberos

- [Finding Feature Information, page 99](#)
- [Prerequisites for Controlling Switch Access with Kerberos, page 99](#)
- [Information about Kerberos, page 100](#)
- [How to Configure Kerberos, page 104](#)
- [Monitoring the Kerberos Configuration, page 104](#)
- [Additional References, page 104](#)

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.
- The Kerberos instance name *must* be in all lowercase characters.
- The Kerberos realm name *must* be in all uppercase characters.

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 and in the *Cisco IOS Security Command Reference, Release 12.4*, the trusted third party can be a Catalyst 3750-E or 3560-E 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 a Catalyst 3750-E or 3560-E Catalyst 3750-X or 3560-X 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 13: Kerberos Terms

Term	Definition
Authentication	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.
Authorization	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.
Credential	A general term that refers to authentication tickets, such as TGTs ² 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.
Instance	<p>An authorization level label for Kerberos principals. Most Kerberos principals are of the form <i>user@REALM</i> (for example, <i>smith@EXAMPLE.COM</i>). A Kerberos principal with a Kerberos instance has the form <i>user/instance@REALM</i> (for example, <i>smith/admin@EXAMPLE.COM</i>). 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.</p> <p>Note The Kerberos principal and instance names <i>must</i> be in all lowercase characters.</p> <p>Note The Kerberos realm name <i>must</i> be in all uppercase characters.</p>
KDC ³	Key distribution center that consists of a Kerberos server and database program that is running on a network host.
Kerberized	A term that describes applications and services that have been modified to support the Kerberos credential infrastructure.

Term	Definition
Kerberos realm	<p>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.</p> <p>Note The Kerberos realm name <i>must</i> be in all uppercase characters.</p>
Kerberos server	<p>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.</p>
KEYTAB ⁴	<p>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 SRVTAB⁵.</p>
Principal	<p>Also known as a Kerberos identity, this is who you are or what a service is according to the Kerberos server.</p> <p>Note The Kerberos principal name <i>must</i> be in all lowercase characters.</p>
Service credential	<p>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.</p>
SRVTAB	<p>A password that a network service shares with the KDC. In Kerberos 5 or later Kerberos versions, SRVTAB is referred to as KEYTAB.</p>
TGT	<p>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.</p>

- ² ticket granting ticket
- ³ key distribution center
- ⁴ key table
- ⁵ server table

Kerberos Operation

A Kerberos server can be a Catalyst 3750-E or 3560-E Catalyst 3750-X or 3560-X controller 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 Catalyst 3750-E or 3560-E Catalyst 3750-X or 3560-X controller as a Kerberos server, remote users must follow these steps:

- 1 [Authenticating to a Boundary Switch, on page 103](#)
- 2 [Obtaining a TGT from a KDC, on page 103](#)
- 3 [Authenticating to Network Services, on page 104](#)

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.
 - 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.

For instructions, see the “Kerberos Configuration Task List” section in the “Security Server Protocols” chapter of the *Cisco IOS Security Configuration Guide, Release 12.4*.

Monitoring the Kerberos Configuration

To display the Kerberos configuration, use the **show running-config** privileged EXEC command.

Additional References

Related Documents

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.html
Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850-library.html
Kerberos Commands	<i>Cisco IOS Security Command Reference, Release 12.4</i>
Kerberos Configuration Examples	<i>Cisco IOS Security Configuration Guide, Release 12.4.</i>

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

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support



Configuring Local Authentication and Authorization

- [Finding Feature Information, page 107](#)
- [How to Configure Local Authentication and Authorization, page 107](#)
- [Monitoring Local Authentication and Authorization, page 110](#)
- [Additional References, page 110](#)

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default local**
5. **aaa authorization exec local**
6. **aaa authorization network local**
7. **username *name* [*privilege level*] {password *encryption-type password*}**
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	aaa new-model Example: SwitchController(config)# aaa new-model	Enables AAA.
Step 4	aaa authentication login default local Example: SwitchController(config)# 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.

	Command or Action	Purpose
Step 5	aaa authorization exec local Example: <pre>SwitchController(config)# aaa authorization exec local</pre>	Configures user AAA authorization, check the local database, and allow the user to run an EXEC shell.
Step 6	aaa authorization network local Example: <pre>SwitchController(config)# aaa authorization network local</pre>	Configures user AAA authorization for all network-related service requests.
Step 7	username name [privilege level] {password encryption-type password} Example: <pre>SwitchController(config) # username your_user_name privilege 1 password 7 secret567</pre>	<p>Enters the local database, and establishes a username-based authentication system.</p> <p>Repeat this command for each user.</p> <ul style="list-style-type: none"> For <i>name</i>, specify the user ID as one word. Spaces and quotation marks are not allowed. (Optional) For <i>level</i>, 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 <i>encryption-type</i>, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows. For <i>password</i>, 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: <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 9	show running-config Example: <pre>SwitchController# show running-config</pre>	Verifies your entries.

	Command or Action	Purpose
Step 10	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

- [SSH Servers, Integrated Clients, and Supported Versions, on page 133](#)
- [TACACS+ and Switch Access, on page 45](#)
- [RADIUS and Switch Access, on page 63](#)
- [Setting Up the SwitchController to Run SSH, on page 135](#)
- [SSH Configuration Guidelines, on page 133](#)

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

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

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/support</p>



Configuring Local Authentication

- [Information About Local Web Authentication, page 113](#)
- [Restrictions for Local Web Authentication, page 114](#)
- [Configuring Local Web Authentication, page 115](#)
- [Monitoring Local Web Authentication, page 126](#)
- [Examples: Local Web Authentication Configuration, page 126](#)
- [Additional References for Configuring the Local Web Authentication Configuration, page 128](#)
- [Feature History for Performing Local Web Authentication Configuration, page 129](#)

Information About Local Web Authentication

Web authentication is a Layer 3 security feature that causes the controller not to allow IP traffic (except DHCP and DNS-related packets) from a particular client until that client has correctly supplied a valid username and password. It is a simple authentication method without the requirement for a supplicant or client utility. Web authentication is typically used by customers who want to deploy a guest-access network. Typical deployments can include hot spot locations such as T-Mobile or Starbucks.

Web authentication does not provide data encryption. Web authentication is typically used as simple guest access for either a hot spot or a campus atmosphere where the only concern is the connectivity.

Web authentication can be performed using:

- Default login window on the controller.
- Modified version of the default login window on the controller.
- A customized login window that you configure on an external web server (external web authentication).
- A customized login window that you download to the controller.

Web Authentication Process

The following process takes place when a user connects to a WLAN configured for web authentication:

- The user opens a web browser and enters a URL, for example, <http://www.cisco.com>. The client sends out a DNS request for this URL to get the IP address for the destination. The controller bypasses the

DNS request to the DNS server and the DNS server responds back with a DNS reply, which contains the IP address of the destination <http://www.cisco.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 <http://www.cisco.com>.
- The controller has rules configured for the client and hence can act as a proxy for <http://www.cisco.com>. It sends back a TCP SYN-ACK packet to the client with source as the IP address of <http://www.cisco.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 <http://www.cisco.com>. The controller intercepts this packet and sends it for redirection handling. The HTTP application gateway prepares a 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 URL of the controller, for example, <http://<Virtual-Server-IP>/login.html>.
- The client closes the TCP connection with the IP address, for example, <http://www.cisco.com>.
- Now the client wishes to navigate to <http://1.1.1.1/login.html>. Therefore, the client tries to open a TCP connection with the virtual IP address of the controller. It sends a TCP SYN packet for 1.1.1.1 to the controller.
- The controller responds back with a TCP SYN-ACK and the client sends back a TCP ACK to the WLC in order to complete the handshake.
- The client sends a HTTP GET for /login.html destined to 1.1.1.1 in order to request for the login page.
- This request is allowed based on the web server configured for the controller and the server responds back with the default login page. The client receives the login page on the browser window where the user can log in.

Restrictions for Local Web Authentication

- Sometimes clients are dropped in the IP learn state. To prevent clients from dropping, make sure you enable IP DHCP snooping globally and for the client VLAN.
- Some devices (For example, Ipads) may not redirect to the login page if IP HTTP secure server is used.
- If you have enabled the secure server using the **ip http secure-server** command and then disable it using the **no** form of the command, you need to reboot the controller for the secure server to get deactivated.

Configuring Local Web Authentication

Configuring Local Web Authentication for Local Net Users Using AAA (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login** *local_webauth local*
3. **aaa authorization network** *local_webauth local*
4. **aaa authorization network** *default local*
5. **aaa authorization credential-download** *default local*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 2	aaa authentication login <i>local_webauth local</i> Example: SwitchController(config)# aaa authentication login <i>local_webauth local</i>	Sets an authentication method list <i>local_webauth</i> to the group type <i>local</i> .
Step 3	aaa authorization network <i>local_webauth local</i> Example: SwitchController(config)# aaa authorization network <i>local_webauth local</i>	Sets an authorization method list <i>local_webauth</i> to the group type <i>local</i> .
Step 4	aaa authorization network <i>default local</i> Example: SwitchController(config)# aaa authorization network default local	Sets an authorization method list for local user.
Step 5	aaa authorization credential-download <i>default local</i> Example: SwitchController(config)# aaa authorization credential-download default local	Sets an authorization method list for use of local credentials.

Configuring Local Web Authentication Using RADIUS Server (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login** *authentication-list-name* **group** *radius-server-group*
3. **aaa authorization network** *authentication-list-name* **group** *radius-server-group*
4. **aaa group server radius** *radius-server-group*
5. **radius server** *server-name*
6. **address ipv4** *ipv4-address* **auth-port** *auth-port-number* **acct-port** *acct-port-number*
7. **key** *ww-wireless*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 2	aaa authentication login <i>authentication-list-name</i> group <i>radius-server-group</i> Example: SwitchController(config)# aaa authentication login webauth_radius group ISE_group	Sets an authentication method list to the RADIUS server group.
Step 3	aaa authorization network <i>authentication-list-name</i> group <i>radius-server-group</i> Example: SwitchController(config)# aaa authorization network webauth_radius group ISE_group	Sets an authorization method list to the RADIUS server group.
Step 4	aaa group server radius <i>radius-server-group</i> Example: SwitchController(config)# aaa group server radius ISE_Group	Sets an RADIUS server group.
Step 5	radius server <i>server-name</i> Example: SwitchController(config)# radius server ISE	Sets an RADIUS server.
Step 6	address ipv4 <i>ipv4-address</i> auth-port <i>auth-port-number</i> acct-port <i>acct-port-number</i> Example: SwitchController(config-radius-server)# address ipv4 192.168.154.119 auth-port 1812 acct-port 1813	Sets an RADIUS server.

	Command or Action	Purpose
Step 7	key ww-wireless Example: SwitchController(config-radius-server)# key ww-wireless	Sets an RADIUS server encryption key.

Configuring Local Web Authentication Using RADIUS Server (GUI)

-
- Step 1** Choose **Configuration > Security > AAA > Method Lists > Authentication** to open the **Authentication** page.
- Step 2** Click **New** to open the **Authentication > New** page.
- Step 3** In the **Method List name** text box, enter the name for new method list, for example, **webauth_radius** for RADIUS server.
- Step 4** In the **Type** field, choose **login**.
- Step 5** In the **Group Type** field, choose **group**.
- Step 6** Select the RADIUS server group from the **Available Server Groups** field.
- Step 7** Click **Apply** to save the configuration.
The Authentication method list is displayed in the **Authentication** summary page.
- Step 8** Choose **Configuration > Security > AAA > Method Lists > Authorization** to open the **Authorization** page.
- Step 9** Click **New** to open the **Authorization > New** page.
- Step 10** In the **Method List name** text box, enter the name for new method list, for example, **webauth_radius** for RADIUS server.
- Step 11** In the **Type** field, choose **network**.
- Step 12** In the **Group Type** field, choose **group**.
- Step 13** Select the RADIUS server group from the **Available Server Groups** field.
- Step 14** Click **Apply** to save the configuration.
The Authorization method list is displayed in the **Authorization** summary page.
-

Configuring Guest Users for Local Web Authentication (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **username name { creation-time time | privilege level | password encryption-type password**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example: SwitchController# configure terminal</p>	Enters global configuration mode.
Step 2	<p>username <i>name</i> { creation-time <i>time</i> privilege <i>level</i> password <i>encryption-type</i> <i>password</i></p> <p>Example: SwitchController(config)# user-name viten_webauth creation-time 1368715259 privilege 15 password 0 test12345</p>	<p>Enters the local database, and establishes a username-based authentication system. Repeat this command for each user.</p> <ul style="list-style-type: none"> • For name, specify the user ID as one word. Spaces and quotation marks are not allowed. • (Optional) For level, specify the privilege level the user has after gaining access. The range is 0 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.

Configuring Guest Users for Local Web Authentication (GUI)

-
- Step 1** Choose **Configuration > Security > RADIUS > Users** to open the **AAA Users** page.
- Step 2** In the **User Name** text box, enter the username.
For name, specify the user ID as one word. Spaces and quotation marks are not allowed.
- Step 3** In the **Privilege** drop-down list, choose 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. Enter 7 to specify that a hidden password follows.
- Step 4** In the **Password** text box, enter the password the user must enter to gain access to the controller.
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 5** In the **Confirm Password** text box, enter the password again.
- Step 6** In the **Type** drop-down list, choose the type of user, for example, **network-user**.
- Step 7** Check the **Guest User** checkbox.
- Step 8** Check the **Set Validity** checkbox (optional).
- Step 9** From the **Lifetime** drop-down list, choose the validity period of the user (optional).
- Step 10** Click **Apply** to save the configuration.
-

Configuring a Parameter Map for Local Web Authentication (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **parameter-map type webauth global**
3. **banner** *{file | text}*
4. **custom-page**
5. **max-http-conns**
6. **intercept-https-enable**
7. **ratelimit**
8. **redirect**
9. **timeout**
10. **watch-list**
11. **virtual-ip ipv4** *virtual -IP-address*
12. **exit**
13. **no**
14. **parameter-map type webauth** *name type webauth test*
15. **banner** *bannet-text*
16. **consent email**
17. **custom-page**
18. **max-http-conns**
19. **redirect**
20. **timeout**
21. **type**
22. **exit**
23. **no**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 2	parameter-map type webauth global Example: SwitchController(config)# parameter-map type webauth global	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.
Step 3	banner {file text} Example: SwitchController(config-params-parameter-map) # banner	Displays a banner on the local web-authentication login web page.
Step 4	custom-page Example: SwitchController(config-params-parameter-map) # custom-page	Specifies the custom page such as login, expired, success, or failure page.
Step 5	max-http-conns Example: SwitchController(config-params-parameter-map) # max-http-conns	Specifies the maximum number of HTTP connections per clients.
Step 6	intercept-https-enable Example: SwitchController(config-params-parameter-map) # intercept-https-enable	Specifies to enable intercept of HTTPS traffic.
Step 7	ratelimit Example: SwitchController(config-params-parameter-map) # ratelimit	Specifies to rate limit on the number of web authentication sessions.
Step 8	redirect Example: SwitchController(config-params-parameter-map) # redirect	Specifies to redirect the URL.
Step 9	timeout Example: SwitchController(config-params-parameter-map) # timeout	Specifies to timeout for the initial state of web authentication.

	Command or Action	Purpose
Step 10	watch-list Example: SwitchController(config-params-parameter-map) # watch-list	Specifies the watch list of web authentication clients.
Step 11	virtual-ip ipv4 virtual -IP-address Example: SwitchController(config-params-parameter-map) # virtual-ip ipv4 172.16.16.16	(Optional) Specifies a virtual IP address for web-based authentication clients. This command is supported in the global parameter map only.
Step 12	exit Example: SwitchController(config-params-parameter-map) # exit	Specifies to exit from parameter-map params configuration mode.
Step 13	no Example: SwitchController(config-params-parameter-map) # no	Specifies to negate a command or set its defaults.
Step 14	parameter-map type webauth name type webauth test Example: SwitchController(config) # parameter-map type webauth user1 type webauth test	Specifies parameter map user-defined name for local web-based authentication clients. This command is supported in the global parameter map only.
Step 15	banner bannet-text Example: SwitchController(config-params-parameter-map) # banner	(Optional) Displays a banner on the local web-authentication login web page.
Step 16	consent email Example: SwitchController(config-params-parameter-map) # consent email	(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.
Step 17	custom-page Example: SwitchController(config-params-parameter-map) # custom-page	Specifies the custom page such as login, expired, success, or failure page.
Step 18	max-http-conns Example: SwitchController(config-params-parameter-map) # max-http-conns	Specifies the maximum number of HTTP connections per clients.

	Command or Action	Purpose
Step 19	redirect Example: SwitchController (config-params-parameter-map) # redirect	Specifies to redirect the URL.
Step 20	timeout Example: SwitchController (config-params-parameter-map) # timeout	Specifies to timeout for the initial state of web authentication.
Step 21	type Example: SwitchController (config-params-parameter-map) # virtual-ip ipv4 172.16.16.16	(Optional) Specifies the parameter type such as web authentication or consent, or both.
Step 22	exit Example: SwitchController (config-params-parameter-map) # exit	Specifies to exit from parameter-map params configuration mode.
Step 23	no Example: SwitchController (config-params-parameter-map) # no	Specifies to negate a command or set its defaults.

Configuring a Parameter Map and Method List for Local Web Authentication (GUI)

-
- Step 1** Create a global parameter map:
- Choose **Configuration > Security > Web Auth > Webauth Parameter Map** to open the **Webauth Parameter Map** page.
 - Click the **global** parameter map.
 - In the **Virtual IPv4 Address** text box, enter the virtual IPv4 address.
 - Click **Apply** to save the configuration.
- Step 2** Create a new parameter map:
- Choose **Configuration > Security > Web Auth > Webauth Parameter Map** to open the **Webauth Parameter Map** page.
 - Click **New** to open the **Webauth Parameter Map** page.
 - In the **Parameter-map name**, enter the name for the parameter map.

- d) From the **Type - web-auth, consent or both**, choose **webauth**.
- e) Click **Apply** to save the configuration.

Step 3

Create authentication method list for local users for local authentication:

- a) Choose **Configuration > Security > AAA > Method Lists > Authentication** to open the **Authentication** page.
- b) Click **New** to open the **Authentication > New** page.
- c) In the **Method List name** text box, enter the name for new method list, for example, **local_webauth** for AAA server.
- d) In the **Type** field, choose **network**.
- e) In the **Group Type** field, choose **local**.
- f) Click **Apply** to save the configuration.

Step 4

Create authentication method list for RADIUS authentication:

- a) Choose **Configuration > Security > AAA > Method Lists > Authentication** to open the **Authentication** page.
- b) Click **New** to open the **Authentication > New** page.
- c) In the **Method List name** text box, enter the name for new method list, for example, **webauth_radius** for radius authentication.
- d) In the **Type** field, choose **login**.
- e) In the **Group Type** field, choose **group**.
- f) In the **Groups In This Method** section, select the RADIUS server group, and move it from the **Available Server Groups** area to the **Assigned Server Groups** area.
- g) Click **Apply** to save the configuration.

Step 5

Create authorization method list for local users:

- a) Choose **Configuration > Security > AAA > Method Lists > Authorization** to open the **Authorization** page.
- b) Click **New** to open the **Authorization > New** page.
- c) In the **Method List name** text box, enter the name for new method list, for example, **local_webauth**.
- d) In the **Type** field, choose **network**.
- e) In the **Group Type** field, choose **local**.
- f) Click **Apply** to save the configuration.

Step 6

Create another authorization method list for local authentication:

- a) Choose **Configuration > Security > AAA > Method Lists > Authorization** to open the **Authorization** page.
- b) Click **New** to open the **Authorization > New** page.
- c) In the **Method List name** text box, enter **default**.
- d) In the **Type** field, choose **credential-download**.
- e) In the **Group Type** field, choose **local**.
- f) Click **Apply** to save the configuration.
- g) The **Authorization** page lists the method lists that include default and local web_auth method lists.

Step 7

Create authorization method list for RADIUS authentication:

- a) Choose **Configuration > Security > AAA > Method Lists > Authorization** to open the **Authorization** page.
- b) Click **New** to open the **Authentication > New** page.
- c) In the **Method List name** text box, enter the name for new method list, for example, **webauth_radius** for radius authentication.
- d) In the **Type** field, choose **network**.
- e) In the **Group Type** field, choose **group**.
- f) In the **Groups In This Method** section, select the RADIUS server group, and move it from the **Available Server Groups** area to the **Assigned Server Groups** area.

g) Click **Apply** to save the configuration.

Configuring Local Web Authentication on a WLAN (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *wlan-name wlan-id ssid/network-name*
3. **client vlan** *wlan-name wlan-id/vlan-name*
4. **no security wpa**
5. **no security wpa akm dot1x**
6. **no security wpa wpa2**
7. **no security wpa wpa2 ciphers aes**
8. **security web-auth**
9. **security web-auth authentication-list** *authentication-list-name*
10. **security web-auth parameter-map** *parameter-map name*
11. **session-timeout** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 2	wlan <i>wlan-name wlan-id ssid/network-name</i> Example: SwitchController(config)# wlan user_webauth 7 user_webauth	Configures WLAN network.
Step 3	client vlan <i>wlan-name wlan-id/vlan-name</i> Example: SwitchController(config-wlan)# client vlan user1	Enters into VLAN configuration mode.
Step 4	no security wpa Example: SwitchController(config-wlan)# no security wpa	Disables WPA or WPA2 support for a WLAN.

	Command or Action	Purpose
Step 5	no security wpa akm dot1x Example: SwitchController(config-wlan)# no security wpa akm dot1x	Disables WPA or WPA2 auth key management 802.1x support for a WLAN.
Step 6	no security wpa wpa2 Example: SwitchController(config-wlan)# no security wpa wpa2	Disables WPA2 support for a WLAN.
Step 7	no security wpa wpa2 ciphers aes Example: SwitchController(config-wlan)# no security wpa wpa2 ciphers aes	Disables WPA2 ciphers for a WLAN.
Step 8	security web-auth Example: SwitchController(config-wlan)# security web-auth	Sets the SSID to security web authentication.
Step 9	security web-auth authentication-list authentication-list-name Example: Local web Auth using AAA Server: SwitchController(config-wlan)# security web-auth authentication-list local_webauth Local web Auth using RADIUS Server: SwitchController(config-wlan)# security web-auth authentication-list webauth_radius	Allows you to map the authentication list name from AAA server or RADIUS server within a WLAN.
Step 10	security web-auth parameter-map parameter-map name Example: Using Parameter map from AAA server: SwitchController(config-wlan)# security web-auth parameter-map vit_web Using Parameter map from RADIUS server: SwitchController(config-wlan)# security web-auth parameter-map webauth_radius	Allows you to map the parameter-map name with the web-auth WLAN.
Step 11	session-timeout seconds Example: SwitchController(config-wlan)# session-timeout 1800	Configures session timeout for clients associated to a WLAN. A value of zero (0) is equivalent to no timeout. The range is from 300 to 86400.

Configuring Local Web Authentication on a WLAN (GUI)

-
- Step 1** Choose **Configuration > WLANs > New** to open the **WLAN > New** page.
- Step 2** Choose **Security > Layer 3** in the **WLAN > Edit** page.
- Step 3** Check the **Web Policy** checkbox.
- Step 4** In the **Webauth Profile** text box, enter the name of the web auth profile, for example, `local_webauth` or `webauth_radius`.
- Step 5** From the **Webauth Parameter Map** drop-down list, choose the web auth parameter you have created, for example, `test_web`.
- Step 6** Click **Apply** to save the configuration.
Note Do not configure the AAA server.
- Step 7** Choose **Monitor > Clients** to open the **Clients > Detail** page to view the client details for an authenticated user.
-

Monitoring Local Web Authentication

The following commands can be used to monitor local web authentication configured on the controller.

Table 14: Monitoring Local Web Authentication Command

Command	Purpose
<code>show running-config aaa</code>	Displays the AAA configuration in the running configuration.
<code>show run section parameter</code>	Displays the section parameter details in the running configuration.
<code>show wireless client mac-address mac-address detail</code>	Displays detailed information of wireless client based on its MAC address.

Examples: Local Web Authentication Configuration

This example shows how to configure local web authentication for local net users using AAA:

```
SwitchController# config terminal
SwitchController(config)# aaa authentication login local_webauth local
SwitchController(config)# aaa authorization network local_webauth local
SwitchController(config)# aaa authorization credential-download default local
SwitchController(config)# end
SwitchController# show run aaa
```

This example shows how to configure local web authentication for local net users using RADIUS server:

```
SwitchController# config terminal
SwitchController(config)# aaa authentication login webauth_radius group ISE_group
SwitchController(config)# aaa authorization network webauth_radius group ISE_group
SwitchController(config)# aaa group server radius ISE_Group
SwitchController(config)# radius server ISE
SwitchController(config-radius-server)# address ipv4 192.168.154.119 auth-port 1812 acct-port
1813
SwitchController(config-radius-server)# key ww-wireless
SwitchController(config-radius-server)# end
SwitchController# show run aaa
```

This example shows how to configure guest users for local web authentication:

```
SwitchController# config terminal
SwitchController(config)# user-name viten_webauth creation-time 1368715259 privilege 15
password 0 test12345
SwitchController(config)# end
```

This example shows how to configure parameter map for local web authentication using AAA:

```
SwitchController# config terminal
SwitchController(config)# parameter-map type webauth global
SwitchController(config-params-parameter-map)# virtual-ip ipv4 172.16.16.16
SwitchController(config-params-parameter-map)# parameter-map type webauth user1 type webauth
test
SwitchController(config-params-parameter-map)# banner
SwitchController(config-params-parameter-map)# end
SwitchController# show run aaa
```

This example shows how to configure local web authentication on a WLAN using AAA:

```
SwitchController# config terminal
SwitchController(config)# wlan user_webauth 7 user_webauth
SwitchController(config-wlan)# client vlan user1
SwitchController(config-wlan)# no security wpa
SwitchController(config-wlan)# no security wpa akm dot1x
SwitchController(config-wlan)# no security wpa wpa2
SwitchController(config-wlan)# no security wpa wpa2 ciphers aes
SwitchController(config-wlan)# security web-auth
SwitchController(config-wlan)# security web-auth authentication-list local_webauth
SwitchController(config-wlan)# security web-auth parameter-map vit_web
SwitchController(config-wlan)# session-timeout 1800
SwitchController(config-wlan)# end
SwitchController# show run aaa
```

This example shows how to configure local web authentication on a WLAN using RADIUS server:

```
SwitchController# config terminal
SwitchController(config)# wlan user_webauth 7 user_webauth
SwitchController(config-wlan)# client vlan user1
SwitchController(config-wlan)# no security wpa
SwitchController(config-wlan)# no security wpa akm dot1x
SwitchController(config-wlan)# no security wpa wpa2
SwitchController(config-wlan)# no security wpa wpa2 ciphers aes
SwitchController(config-wlan)# security web-auth
SwitchController(config-wlan)# security web-auth authentication-list webauth_radius
SwitchController(config-wlan)# security web-auth parameter-map webauth_radius
SwitchController(config-wlan)# session-timeout 1800
SwitchController(config-wlan)# end
SwitchController# show run aaa
```

Additional References for Configuring the Local Web Authentication Configuration

Related Documents

Related Topic	Document Title
Security commands	<i>Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>
Local web authentication configuration example	<i>WLC 5760/3850 Custom WebAuth with Local Authentication Configuration Example</i>

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History for Performing Local Web Authentication Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.



Configuring Secure Shell (SSH)

- [Finding Feature Information, page 131](#)
- [Prerequisites for Configuring the Switch for Secure Shell \(SSH\) and Secure Copy Protocol \(SCP\), page 131](#)
- [Restrictions for Configuring the SwitchController for SSH, page 132](#)
- [Information about SSH, page 132](#)
- [How to Configure SSH, page 135](#)
- [Monitoring the SSH Configuration and Status, page 139](#)
- [Additional References, page 139](#)

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 the Switch for Secure Shell (SSH) and Secure Copy Protocol (SCP)

The following are the prerequisites for configuring the switch for secure shell (SSH):

- To use SSH, you must install the cryptographic (encrypted) software image on your switch.
- For SSH to work, the switch needs an 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.
- A user must have appropriate authorization to use SCP.
- A user who has appropriate authorization can use SCP to copy any file in the Cisco IOS File System (IFS) to and from a switch by using the **copy** command. An authorized administrator can also do this from a workstation.

Related Topics

[Secure Copy Protocol, on page 134](#)

Restrictions for Configuring the SwitchController for SSH

The following are restrictions for configuring the SwitchController 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 DES (56-bit) and 3DES (168-bit) data encryption software.
- The SwitchController 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.
- This software release does not support IP Security (IPSec).
- When using SCP, you cannot enter the password into the **copy** command. You must enter the password when prompted.

Related Topics

[Secure Copy Protocol, on page 134](#)

Information about SSH

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 SSH feature has an SSH server and an SSH integrated client, which are applications that run on the switch. You can use an SSH client to connect to a switch running the SSH server. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client also works with the SSH server supported in this release and with non-Cisco SSH servers.

The switch supports an SSHv1 or an SSHv2 server.

The switch supports an SSHv1 client.

SSH supports the Data Encryption Standard (DES) encryption algorithm, the Triple DES (3DES) encryption algorithm, and password-based user authentication.

SSH also supports these user authentication methods:

- TACACS+
- RADIUS
- Local authentication and authorization

Related Topics

[Configuring the Switch for Local Authentication and Authorization, on page 107](#)

[TACACS+ and Switch Access, on page 45](#)

[RADIUS and Switch Access, on page 63](#)

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 SwitchController to Run SSH, on page 135](#)

[Configuring the Switch for Local Authentication and Authorization, on page 107](#)

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

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying controller 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 controller 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 the Switch for Secure Shell \(SSH\) and Secure Copy Protocol \(SCP\), on page 131](#)

[Restrictions for Configuring the SwitchController for SSH, on page 132](#)

How to Configure SSH

Setting Up the SwitchController to Run SSH

Follow these steps to set up your SwitchController 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname *hostname***
4. **ip domain-name *domain_name***
5. **crypto key generate rsa**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	hostname <i>hostname</i> Example: SwitchController(config)# hostname your_hostname	Configures a hostname and IP domain name for your SwitchController. Note Follow this procedure only if you are configuring the SwitchController as an SSH server.

	Command or Action	Purpose
Step 4	ip domain-name <i>domain_name</i> Example: <pre>SwitchController(config)# ip domain-name your_domain</pre>	Configures a host domain for your SwitchController.
Step 5	crypto key generate rsa Example: <pre>SwitchController(config)# crypto key generate rsa</pre>	<p>Enables the SSH server for local and remote authentication on the SwitchController and generates an RSA key pair. Generating an RSA key pair for the SwitchController automatically enables SSH.</p> <p>We recommend that a minimum modulus size of 1024 bits.</p> <p>When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.</p> <p>Note Follow this procedure only if you are configuring the SwitchController as an SSH server.</p>
Step 6	end Example: <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 7	show running-config Example: <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 8	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

[SSH Configuration Guidelines, on page 133](#)

[Configuring the Switch for Local Authentication and Authorization, on page 107](#)

Configuring the SSH Server

Follow these steps to configure the SSH server:



Note This procedure is only required if you are configuring the SwitchController as an SSH server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ssh version [1 | 2]**
4. **ip ssh {timeout *seconds* | authentication-retries *number*}**
5. Use one or both of the following:
 - **line vtyline_number[ending_line_number]**
 - **transport input ssh**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	ip ssh version [1 2] Example: SwitchController(config)# ip ssh version 1	(Optional) Configures the SwitchController to run SSH Version 1 or SSH Version 2. <ul style="list-style-type: none"> • 1—Configure the SwitchController to run SSH Version 1. • 2—Configure the SwitchController to run 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 4	ip ssh {timeout <i>seconds</i> authentication-retries <i>number</i>}	Configures the SSH control parameters:

	Command or Action	Purpose
	<p>Example:</p> <pre>SwitchController(config)# ip ssh timeout 90 authentication-retries 2</pre>	<ul style="list-style-type: none"> 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 SwitchController 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. <p>Repeat this step when configuring both parameters.</p>
Step 5	<p>Use one or both of the following:</p> <ul style="list-style-type: none"> line <code>vt</code><i>line_number</i> [<i>ending_line_number</i>] transport input ssh <p>Example:</p> <pre>SwitchController(config)# line vty 1 10</pre> <p>or</p> <pre>SwitchController(config-line)# transport input ssh</pre>	<p>(Optional) Configures the virtual terminal line settings.</p> <ul style="list-style-type: none"> Enters line configuration mode to configure the virtual terminal line settings. For <i>line_number</i> and <i>ending_line_number</i>, specify a pair of lines. The range is 0 to 15. Specifies that the SwitchController prevent non-SSH Telnet connections. This limits the router to only SSH connections.
Step 6	<p>end</p> <p>Example:</p> <pre>SwitchController(config-line)# end</pre>	Returns to privileged EXEC mode.
Step 7	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 8	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Monitoring the SSH Configuration and Status

This table displays the SSH server configuration and status.

Table 15: Commands for Displaying the SSH Server Configuration and Status

Command	Purpose
<code>show ip ssh</code>	Shows the version and configuration information for the SSH server.
<code>show ssh</code>	Shows the status of the SSH server.

Additional References

Related Documents

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.html
Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850-library.html

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

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support



CHAPTER 11

Configuring Secure Socket Layer HTTP

- [Finding Feature Information, page 141](#)
- [Information about Secure Sockets Layer \(SSL\) HTTP, page 141](#)
- [How to Configure Secure HTTP Servers and Clients, page 144](#)
- [Monitoring Secure HTTP Server and Client Status, page 150](#)
- [Additional References, page 151](#)

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.

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.



Note

The certificate authorities and trustpoints must be configured on each device individually. Copying them from other devices makes them invalid on the switch.

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.

```
SwitchController# 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 6174652D 33303830 37353530 37323126 30240609 2A864886 F70D0109
02161743 45322D33 3535302D 31332E73 756D6D30 342D3335 3530301E 170D3933
30333031 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-30890755072** 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.

For additional information on Certificate Authorities, see the “Configuring Certification Authority Interoperability” chapter in the *Cisco IOS Security Configuration Guide, Release 12.4*.

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_RC4_128_MD5`—RSA key exchange with RC4 128-bit encryption and MD5 for message digest
- 3 `SSL_RSA_WITH_RC4_128_SHA`—RSA key exchange with RC4 128-bit encryption and SHA for message digest
- 4 `SSL_RSA_WITH_3DES_EDE_CBC_SHA`—RSA key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest

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:

SUMMARY STEPS

1. **configure terminal**
2. **hostname** *hostname*
3. **ip domain-name** *domain-name*
4. **crypto key generate rsa**
5. **crypto ca trustpoint** *name*
6. **enrollment url** *url*
7. **enrollment http-proxy** *host-name port-number*
8. **crl query** *url*
9. **primary** *name*
10. **exit**
11. **crypto ca authentication** *name*
12. **crypto ca enroll** *name*
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	hostname <i>hostname</i> Example: SwitchController(config)# hostname your_hostname	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.
Step 3	ip domain-name <i>domain-name</i> Example: SwitchController(config)# ip domain-name your_domain	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.
Step 4	crypto key generate rsa Example: SwitchController(config)# crypto key generate rsa	(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.
Step 5	crypto ca trustpoint <i>name</i> Example: SwitchController(config)# crypto ca trustpoint your_trustpoint	Specifies a local configuration name for the CA trustpoint and enter CA trustpoint configuration mode.
Step 6	enrollment url <i>url</i> Example: SwitchController(ca-trustpoint)# enrollment url http://your_server:80	Specifies the URL to which the switch should send certificate requests.
Step 7	enrollment http-proxy <i>host-name port-number</i> Example: SwitchController(ca-trustpoint)# enrollment http-proxy your_host 49	(Optional) Configures the switch to obtain certificates from the CA through an HTTP proxy server. <ul style="list-style-type: none"> • For <i>host-name</i>, specify the proxy server used to get the CA. • For <i>port-number</i>, specify the port number used to access the CA.

	Command or Action	Purpose
Step 8	crl query <i>url</i> Example: SwitchController(ca-trustpoint)# crl query <i>ldap://your_host:49</i>	Configures the switch to request a certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.
Step 9	primary <i>name</i> Example: SwitchController(ca-trustpoint)# primary <i>your_trustpoint</i>	(Optional) Specifies that the trustpoint should be used as the primary (default) trustpoint for CA requests. <ul style="list-style-type: none"> • For <i>name</i>, specify the trustpoint that you just configured.
Step 10	exit Example: SwitchController(ca-trustpoint)# exit	Exits CA trustpoint configuration mode and return to global configuration mode.
Step 11	crypto ca authentication <i>name</i> Example: SwitchController(config)# crypto ca authentication <i>your_trustpoint</i>	Authenticates the CA by getting the public key of the CA. Use the same name used in Step 5.
Step 12	crypto ca enroll <i>name</i> Example: SwitchController(config)# crypto ca enroll <i>your_trustpoint</i>	Obtains the certificate from the specified CA trustpoint. This command requests a signed certificate for each RSA key pair.
Step 13	end Example: SwitchController(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
```

SUMMARY STEPS

1. `show ip http server status`
2. `configure terminal`
3. `ip http secure-server`
4. `ip http secure-port port-number`
5. `ip http secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}`
6. `ip http secure-client-auth`
7. `ip http secure-trustpoint name`
8. `ip http path path-name`
9. `ip http access-class access-list-number`
10. `ip http max-connections value`
11. `ip http timeout-policy idle seconds life seconds requests value`
12. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>show ip http server status</code></p> <p>Example:</p> <pre>SwitchController# show ip http server status</pre>	<p>(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:</p> <pre>HTTP secure server capability: Present</pre> <p>or</p> <pre>HTTP secure server capability: Not present</pre>
Step 2	<p><code>configure terminal</code></p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	<p>Enters global configuration mode.</p>

	Command or Action	Purpose
Step 3	<p>ip http secure-server</p> <p>Example:</p> <pre>SwitchController(config)# ip http secure-server</pre>	Enables the HTTPS server if it has been disabled. The HTTPS server is enabled by default.
Step 4	<p>ip http secure-port <i>port-number</i></p> <p>Example:</p> <pre>SwitchController(config)# ip http secure-port 443</pre>	(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.
Step 5	<p>ip http secure-ciphersuite {[3des-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}</p> <p>Example:</p> <pre>SwitchController(config)# ip http secure-ciphersuite rc4-128-md5</pre>	(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.
Step 6	<p>ip http secure-client-auth</p> <p>Example:</p> <pre>SwitchController(config)# ip http secure-client-auth</pre>	(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.
Step 7	<p>ip http secure-trustpoint <i>name</i></p> <p>Example:</p> <pre>SwitchController(config)# ip http secure-trustpoint your_trustpoint</pre>	Specifies the CA trustpoint to use to get an X.509v3 security certificate and to authenticate the client certificate connection. Note Use of this command assumes you have already configured a CA trustpoint according to the previous procedure.
Step 8	<p>ip http path <i>path-name</i></p> <p>Example:</p> <pre>SwitchController(config)# ip http path /your_server:80</pre>	(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).
Step 9	<p>ip http access-class <i>access-list-number</i></p> <p>Example:</p> <pre>SwitchController(config)# ip http access-class 2</pre>	(Optional) Specifies an access list to use to allow access to the HTTP server.

	Command or Action	Purpose
Step 10	<p>ip http max-connections <i>value</i></p> <p>Example:</p> <pre>SwitchController(config)# ip http max-connections 4</pre>	(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.
Step 11	<p>ip http timeout-policy idle <i>seconds</i> life <i>seconds</i> requests <i>value</i></p> <p>Example:</p> <pre>SwitchController(config)# ip http timeout-policy idle 120 life 240 requests 1</pre>	<p>(Optional) Specifies how long a connection to the HTTP server can remain open under the defined circumstances:</p> <ul style="list-style-type: none"> • 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	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.

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.

SUMMARY STEPS

1. **configure terminal**
2. **ip http client secure-trustpoint** *name*
3. **ip http client secure-ciphersuite** {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	ip http client secure-trustpoint <i>name</i> Example: SwitchController(config)# ip http client secure-trustpoint your_trustpoint	(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.
Step 3	ip http client secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]} Example: SwitchController(config)# ip http client secure-ciphersuite rc4-128-md5	(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.
Step 4	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.

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 16: Commands for Displaying the SSL Secure Server and Client Status

Command	Purpose
show ip http client secure status	Shows the HTTP secure client configuration.
show ip http server secure status	Shows the HTTP secure server configuration.
show running-config	Shows the generated self-signed certificate for secure HTTP connections.

Additional References

Related Documents

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.html
Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850-library.html

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

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/support</p>



Configuring IPv4 ACLs

- [Finding Feature Information, page 153](#)
- [Prerequisites for Configuring Network Security with ACLs, page 153](#)
- [Restrictions for Configuring Network Security with ACLs, page 154](#)
- [Information about Network Security with ACLs, page 155](#)
- [How to Configure ACLs, page 169](#)
- [Monitoring IPv4 ACLs, page 192](#)
- [Configuration Examples for ACLs, page 193](#)
- [Additional References, page 206](#)

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 Network Security with ACLs

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 Network Security with ACLs

General Network Security

The following are restrictions for configuring network security with ACLs:

- Router ACLs and VLAN maps are not supported on switches running the LAN base feature set.
- You cannot apply named MAC extended ACLs to Layer 3 interfaces.
- 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. VLAN maps also accept 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 Filtering

The following are restrictions on ACL filtering:

- If IEEE 802.1Q tunneling is configured on an interface, any IEEE 802.1Q encapsulated IP packets received on the tunnel port can be filtered by MAC ACLs, but not by IP ACLs. This is because the switch does not recognize the protocol inside the IEEE 802.1Q header. This restriction applies to router ACLs, port ACLs, and VLAN maps.

IPv4 ACL Network Interfaces

The following restrictions apply to IPv4 ACLs to network interfaces:

- Apply an ACL only to inbound Layer 2 interfaces. Apply an ACL to either outbound or inbound Layer 3 interfaces.
- On switches running the LAN base feature set, router (Layer 3) ACLs are supported only on SVIs and not on physical interfaces or Layer 3 EtherChannels.
- When controlling access to an interface, you can use a named or numbered ACL.
- If you apply an ACL to a port that is a member of a VLAN, the port ACL takes precedence over an ACL applied to the VLAN interface.
- 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. Incoming packets received on the Layer 2 port are always filtered by the port ACL.
- 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.
- You do not have to enable routing to apply ACLs to Layer 2 interfaces.
- When private VLANs are configured, you can apply router ACLs only on the primary-VLAN SVIs. The ACL is applied to both primary and secondary VLAN Layer 3 traffic.
- When you configure an egress ACL to permit traffic with a particular DSCP value, you must use the original DSCP value instead of a rewritten value.

**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 unreachable** 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.

Related Topics

[Applying an IPv4 ACL to an Interface, on page 182](#)

[IPv4 ACL Interface Considerations, on page 169](#)

[Creating Named MAC Extended ACLs, on page 183](#)

[Applying a MAC ACL to a Layer 2 Interface, on page 185](#)

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.

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. 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.

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.

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:



Note

On switches running the LAN base feature set, router ACLs are supported only on SVIs and VLAN maps are not supported.

- Port ACLs access-control traffic entering a Layer 2 interface. You can apply only one IP access list and one MAC access list to a Layer 2 interface.
- Router ACLs access-control routed traffic between VLANs and are applied to Layer 3 interfaces in a specific direction (inbound or outbound).

ACL Precedence

When VLAN maps, Port ACLs, and router ACLs are configured on the same switch, the filtering precedence, from greatest to least, is port ACL, router ACL, then VLAN map. 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 Network Security with ACLs, on page 154](#)

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 only on outbound and inbound interfaces. The following access lists are supported:

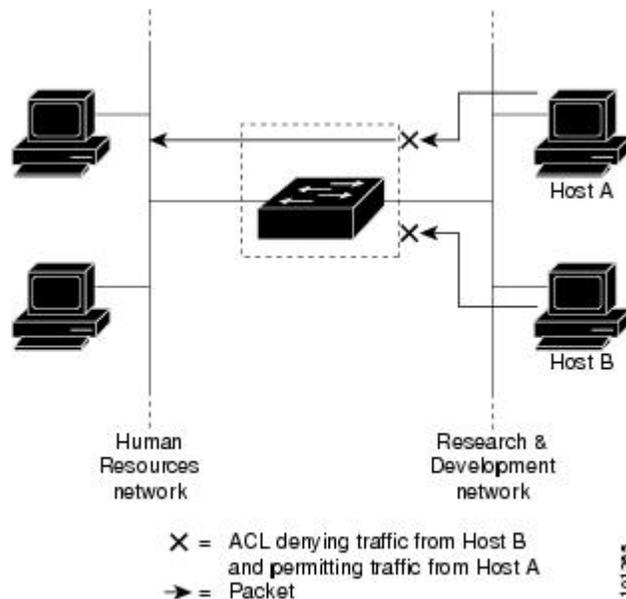
- Standard IP access lists using source addresses
- Extended IP access lists using source and destination addresses and optional protocol type information
- MAC extended access lists using source and destination MAC addresses and optional protocol type information

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.

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.

Figure 3: Using ACLs to Control Traffic in a Network



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.



Note

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.

An ACL can be used with multiple features for a given interface, and one feature can use multiple ACLs. When a single router ACL is used by multiple features, it is examined multiple times.

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. However, you can apply only inbound port ACLs, while router ACLs are supported in both directions. 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

Use VLAN ACLs or VLAN maps to access-control all traffic. You can apply VLAN maps to all packets that are routed into or out of a VLAN or are bridged within a VLAN in the switch or switch stack.

Use VLAN maps for security packet filtering. VLAN maps are not defined by direction (input or output).

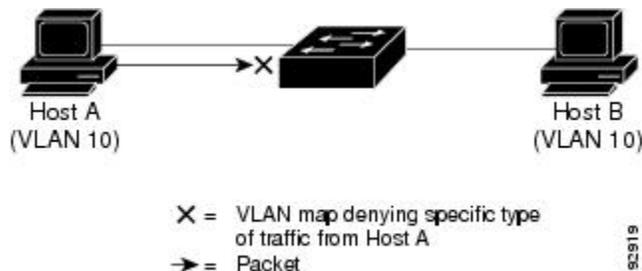
You can configure VLAN maps to match Layer 3 addresses for IPv4 traffic.

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.

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.

Figure 4: Using VLAN Maps to Control Traffic



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.

Example: ACEs and Fragmented and Unfragmented Traffic

Consider access list 102, configured with these commands, applied to three fragmented packets:

```
SwitchController(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
SwitchController(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
SwitchController(config)# access-list 102 permit tcp any host 10.1.1.2
SwitchController(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 switch does not support these Cisco IOS router ACL-related features:

- Non-IP protocol ACLs or bridge-group ACLs
- IP accounting

- Inbound and outbound rate limiting (except with QoS ACLs)
- Reflexive ACLs and dynamic ACLs are not supported. (except for some specialized dynamic ACLs used by the switch clustering feature)
- ACL logging for port ACLs and VLAN maps

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 17: Access List Numbers

Access List Number	Type	Supported
1–99	IP standard access list	Yes
100–199	IP extended access list	Yes
200–299	Protocol type-code access list	No
300–399	DECnet access list	No
400–499	XNS standard access list	No
500–599	XNS extended access list	No
600–699	AppleTalk access list	No
700–799	48-bit MAC address access list	No
800–899	IPX standard access list	No
900–999	IPX extended access list	No
1000–1099	IPX SAP access list	No
1100–1199	Extended 48-bit MAC address access list	No
1200–1299	IPX summary address access list	No
1300–1999	IP standard access list (expanded range)	Yes
2000–2699	IP extended access list (expanded range)	Yes

In addition to numbered standard and extended ACLs, you can also create standard and extended named IP ACLs by using the supported numbers. That is, the name of a standard IP ACL can be 1 to 99; the name of an extended IP ACL can be 100 to 199. The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

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:

These IP protocols are supported:

- Authentication Header Protocol (**ahp**)
- Encapsulation Security Payload (**esp**)
- Enhanced Interior Gateway Routing Protocol (**eigrp**)
- generic routing encapsulation (**gre**)
- Internet Control Message Protocol (**icmp**)
- Internet Group Management Protocol (**igmp**)
- any Interior Protocol (**ip**)
- IP in IP tunneling (**ipinip**)
- KA9Q NOS-compatible IP over IP tunneling (**nos**)
- Open Shortest Path First routing (**ospf**)
- Payload Compression Protocol (**pcp**)
- Protocol-Independent Multicast (**pim**)

- Transmission Control Protocol (**tcp**)
- User Datagram Protocol (**udp**)

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.



Note

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 name of an extended IP ACL can be 100 to 199. 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.
- With IPv4 QoS ACLs, if you enter the **class-map** {**match-all** | **match-any**} *class-map-name* global configuration command, you can enter these **match** commands:

- **match access-group** *acl-name*



Note The ACL must be an extended named ACL.

- **match input-interface** *interface-id-list*

- **match ip dscp** *dscp-list*

- **match ip precedence** *ip-precedence-list*

You cannot enter the **match access-group** *acl-index* command.

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.

**Note**

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.

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.

**Note**

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. Software forwarding of packets might adversely impact the performance of the switch or switch stack, depending on the number of CPU cycles that this consumes.

For router ACLs, other factors can cause packets to be sent to the CPU:

- Using the **log** keyword
- Generating ICMP unreachable messages

When traffic flows are both logged and forwarded, forwarding is done by hardware, but logging must be done by software. Because of the difference in packet handling capacity between hardware and software, if the sum of all flows being logged (both permitted flows and denied flows) is of great enough bandwidth, not all of the packets that are forwarded can be logged.

If router ACL configuration cannot be applied in hardware, packets arriving in a VLAN that must be routed are routed in software, but are bridged in hardware. If ACLs cause large numbers of packets to be sent to the CPU, the switch performance can be negatively affected.

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 access-lists hardware counters** 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 unreachable*s 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

**Note**

VLAN maps are not supported on switches running the LAN base feature set.

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.
- The system might take longer to boot up if you have configured a very large number of ACLs.
- 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.
- You can configure VLAN maps on primary and secondary VLANs. However, we recommend that you configure the same VLAN maps on private-VLAN primary and secondary VLANs.
- When a frame is Layer-2 forwarded within a private VLAN, the same VLAN map is applied at the ingress side and at the egress side. When a frame is routed from inside a private VLAN to an external port, the private-VLAN map is applied at the ingress side.
 - For frames going upstream from a host port to a promiscuous port, the VLAN map configured on the secondary VLAN is applied.
 - For frames going downstream from a promiscuous port to a host port, the VLAN map configured on the primary VLAN is applied.

To filter out specific IP traffic for a private VLAN, you should apply the VLAN map to both the primary and secondary VLANs.

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.

The switch hardware provides one lookup for security ACLs for each direction (input and output); therefore, you must merge a router ACL and a VLAN map when they are configured on the same VLAN. Merging the router ACL with the VLAN map might significantly increase the number of ACEs.

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.

VACL Logging

When you configure VACL logging, syslog messages are generated for denied IP packets under these circumstances:

- When the first matching packet is received.
- For any matching packets received within the last 5 minutes.
- If the threshold is reached before the 5-minute interval.

Log messages are generated on a per-flow basis. A flow is defined as packets with the same IP addresses and Layer 4 (UDP or TCP) port numbers. If a flow does not receive any packets in the 5-minute interval, that flow is removed from the cache. When a syslog message is generated, the timer and packet counter are reset.

VACL logging restrictions:

- Only denied IP packets are logged.
- Packets that require logging on the outbound port ACLs are not logged if they are denied by a VACL.

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 affect in close succession (within a small number of minutes of each other.)

**Note**

The time 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 178](#)

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 182](#)

[Restrictions for Configuring Network Security with ACLs, on page 154](#)

How to Configure ACLs

Configuring IPv4 ACLs

These are the steps to use IP ACLs on the switch:

SUMMARY STEPS

1. Create an ACL by specifying an access list number or name and the access conditions.
2. Apply the ACL to interfaces or terminal lines. You can also apply standard and extended IP ACLs to VLAN maps.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Create an ACL by specifying an access list number or name and the access conditions.	
Step 2	Apply the ACL to interfaces or terminal lines. You can also apply standard and extended IP ACLs to VLAN maps.	

Creating a Numbered Standard ACL

Follow these steps to create a numbered standard ACL:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source source-wildcard* [**log** | **smartlog**]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	access-list <i>access-list-number</i> { deny permit } <i>source source-wildcard</i> [log smartlog] Example: SwitchController(config)# access-list 2 deny your_host	Defines a standard IPv4 access list by using a source address and wildcard. The <i>access-list-number</i> is a decimal number from 1 to 99 or 1300 to 1999. Enter deny or permit to specify whether to deny or permit access if conditions are matched. The <i>source</i> is the source address of the network or host from which the packet is being sent specified as: <ul style="list-style-type: none"> • The 32-bit quantity in dotted-decimal format. • The keyword any as an abbreviation for <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard. • The keyword host as an abbreviation for <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.

	Command or Action	Purpose
		<p>(Optional) The <i>source-wildcard</i> applies wildcard bits to the source.</p> <p>(Optional) Enter log to cause an informational logging message about the packet that matches the entry to be sent to the console.</p> <p>(Optional) Enter smartlog to send copies of denied or permitted packets to a NetFlow collector.</p> <p>Note Logging is supported only on ACLs attached to Layer 3 interfaces. Smart logging is supported only on ACLs attached to Layer 2 interfaces.</p>
Step 4	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 6	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

[Configuring VLAN Maps, on page 187](#)

Creating a Numbered Extended ACL

Follow these steps to create a numbered extended ACL:

SUMMARY STEPS

1. **configure terminal**
2. **access-list** *access-list-number* {deny | permit} *protocol source source-wildcard destination destination-wildcard* [precedence *precedence*] [tos *tos*] [fragments] [log [log-input] | [smartlog]] [time-range *time-range-name*] [dscp *dscp*]
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] | [smartlog]] [time-range *time-range-name*] [dscp *dscp*] [*flag*]
4. **access-list** *access-list-number* {deny | permit} **udp** *source source-wildcard* [operator *port*] *destination destination-wildcard* [operator *port*] [precedence *precedence*] [tos *tos*] [fragments] [log [log-input] | [smartlog]] [time-range *time-range-name*] [dscp *dscp*]
5. **access-list** *access-list-number* {deny | permit} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]]] [precedence *precedence*] [tos *tos*] [fragments] [log [log-input] | [smartlog]] [time-range *time-range-name*] [dscp *dscp*]
6. **access-list** *access-list-number* {deny | permit} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [precedence *precedence*] [tos *tos*] [fragments] [log [log-input] | [smartlog]] [time-range *time-range-name*] [dscp *dscp*]
7. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 2	<p>access-list <i>access-list-number</i> {deny permit} <i>protocol source source-wildcard destination destination-wildcard</i> [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [log [log-input] [smartlog]] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>]</p> <p>Example:</p> <pre>SwitchController(config)# access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log</pre>	<p>Defines an extended IPv4 access list and the access conditions.</p> <p>The <i>access-list-number</i> is a decimal number from 100 to 199 or 2000 to 2699.</p> <p>Enter deny or permit to specify whether to deny or permit the packet if conditions are matched.</p> <p>For <i>protocol</i>, enter the name or number of an P protocol: ahp, eigrp, esp, gre, icmp, igmp, igrp, ip, ipinip, nos, ospf, pcp, pim, tcp, or udp, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword ip.</p> <p>Note This step includes options for most IP protocols. For additional specific parameters for TCP, UDP, ICMP, and IGMP, see the following steps.</p> <p>The <i>source</i> is the number of the network or host from which the packet is sent.</p> <p>The <i>source-wildcard</i> applies wildcard bits to the source.</p> <p>The <i>destination</i> is the network or host number to which the packet is sent.</p> <p>The <i>destination-wildcard</i> applies wildcard bits to the destination.</p>

	Command or Action	Purpose
		<p>Source, source-wildcard, destination, and destination-wildcard can be specified as:</p> <ul style="list-style-type: none"> • 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. <p>The other keywords are optional and have these meanings:</p> <ul style="list-style-type: none"> • 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. • smartlog—Enter when smart logging is globally enabled to have a copy of the denied or permitted packet sent to a NetFlow collector. • time-range—Specify the time-range name. • 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. <p>Note 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.</p>
Step 3	<p>access-list <i>access-list-number</i> {deny permit} tcp <i>source source-wildcard</i> [<i>operator port</i>] <i>destination destination-wildcard</i> [<i>operator port</i>] [established] [precedence precedence] [tos tos] [fragments] [log [log-input]] [smartlog] [time-range time-range-name] [dscp dscp] [<i>flag</i>]</p> <p>Example:</p> <pre>SwitchController(config)# access-list 101 permit tcp any any eq 500</pre>	<p>Defines an extended TCP access list and the access conditions.</p> <p>The parameters are the same as those described for an extended IPv4 ACL, with these exceptions:</p> <p>(Optional) Enter an <i>operator</i> and <i>port</i> to compare source (if positioned after <i>source source-wildcard</i>) or destination (if positioned after <i>destination destination-wildcard</i>) 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).</p> <p>Enter the <i>port</i> 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.</p> <p>The other optional keywords have these meanings:</p> <ul style="list-style-type: none"> • established—Enter to match an established connection. This has the same function as matching on the ack or rst flag.

	Command or Action	Purpose
		<ul style="list-style-type: none"> <i>flag</i>—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	<pre>access-list access-list-number {deny permit} udp source source-wildcard [operator port] destination destination-wildcard [operator port] [precedence precedence] [tos tos] [fragments] [log [log-input] [smartlog] [time-range time-range-name] [dscp dscp]</pre> <p>Example:</p> <pre>SwitchController(config)# access-list 101 permit udp any any eq 100</pre>	<p>(Optional) Defines an extended UDP access list and the access conditions.</p> <p>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 flag and established keywords are not valid for UDP.</p>
Step 5	<pre>access-list access-list-number {deny permit} icmp source source-wildcard destination destination-wildcard [icmp-type [[icmp-type icmp-code] [icmp-message]] [precedence precedence] [tos tos] [fragments] [log [log-input] [smartlog] [time-range time-range-name] [dscp dscp]</pre> <p>Example:</p> <pre>SwitchController(config)# access-list 101 permit icmp any any 200</pre>	<p>Defines an extended ICMP access list and the access conditions.</p> <p>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:</p> <ul style="list-style-type: none"> <i>icmp-type</i>—Enter to filter by ICMP message type, a number from 0 to 255. <i>icmp-code</i>—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255. <i>icmp-message</i>—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name.
Step 6	<pre>access-list access-list-number {deny permit} igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [fragments] [log [log-input] [smartlog] [time-range time-range-name] [dscp dscp]</pre> <p>Example:</p> <pre>SwitchController(config)# access-list 101 permit igmp any any 14</pre>	<p>(Optional) Defines an extended IGMP access list and the access conditions.</p> <p>The IGMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with this optional parameter.</p> <p><i>igmp-type</i>—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.</p>
Step 7	<pre>end</pre> <p>Example:</p> <pre>SwitchController(config)# end</pre>	<p>Returns to privileged EXEC mode.</p>

Related Topics[Configuring VLAN Maps, on page 187](#)

Creating Named Standard ACLs

Follow these steps to create a standard ACL using names:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list standard *name***
4. Use one of the following:
 - **deny** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log** | **smartlog**]
 - **permit** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log** | **smartlog**]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	ip access-list standard <i>name</i> Example: SwitchController(config)# ip access-list standard 20	Defines a standard IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 1 to 99.
Step 4	Use one of the following: <ul style="list-style-type: none"> • deny {<i>source</i> [<i>source-wildcard</i>] host <i>source</i> any} [log smartlog] 	In access-list configuration mode, specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

	Command or Action	Purpose
	<ul style="list-style-type: none"> • permit {<i>source</i> [<i>source-wildcard</i>] host <i>source</i> any} [log smartlog] <p>Example:</p> <pre>SwitchController(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255</pre> <p>or</p> <pre>SwitchController(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0</pre>	<ul style="list-style-type: none"> • host <i>source</i>—A source and source wildcard of <i>source</i> 0.0.0.0. • any—A source and source wildcard of 0.0.0.0 255.255.255.255.
Step 5	<p>end</p> <p>Example:</p> <pre>SwitchController(config-std-nacl)# end</pre>	Returns to privileged EXEC mode.
Step 6	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 7	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Creating Extended Named ACLs

Follow these steps to create an extended ACL using names:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended *name***
4. **{deny | permit} protocol {source [source-wildcard] | host source | any} {destination [destination-wildcard] | host destination | any} [precedence precedence] [tos tos] [established] [log | smartlog] [time-range time-range-name]**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	ip access-list extended <i>name</i> Example: SwitchController(config)# ip access-list extended 150	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.
Step 4	{deny permit} protocol {source [source-wildcard] host source any} {destination [destination-wildcard] host destination any} [precedence precedence] [tos tos] [established] [log smartlog] [time-range time-range-name] Example: SwitchController(config-ext-nacl)# permit 0 any any	In access-list configuration mode, specify the conditions allowed or denied. Use the log keyword to get access list logging messages, including violations. <ul style="list-style-type: none"> • host source—A source and source wildcard of <i>source</i> 0.0.0.0. • host destination—A destination and destination wildcard of <i>destination</i> 0.0.0.0. • any—A source and source wildcard or destination and destination wildcard of 0.0.0.0 255.255.255.255.

	Command or Action	Purpose
Step 5	end Example: SwitchController(config-ext-nacl)# end	Returns to privileged EXEC mode.
Step 6	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 7	copy running-config startup-config Example: SwitchController# 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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **time-range** *time-range-name*
4. Use one of the following:
 - **absolute** [*start time date*] [*end time date*]
 - **periodic** *day-of-the-week hh:mm to [day-of-the-week] hh:mm*
 - **periodic** {*weekdays* | *weekend* | *daily*} *hh:mm to hh:mm*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController(config)# enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	time-range <i>time-range-name</i> Example: SwitchController(config)# time-range <i>workhours</i>	Assigns a meaningful name (for example, <i>workhours</i>) 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.
Step 4	Use one of the following: <ul style="list-style-type: none"> • absolute [<i>start time date</i>] [<i>end time date</i>] • periodic <i>day-of-the-week hh:mm to [day-of-the-week] hh:mm</i> • periodic {<i>weekdays</i> <i>weekend</i> <i>daily</i>} <i>hh:mm to hh:mm</i> 	Specifies when the function it will be applied to is operational. <ul style="list-style-type: none"> • You can use only one absolute statement in the time range. If you configure more than one absolute statement, only the one configured last is executed. • You can enter multiple periodic statements. For example, you could configure different hours for weekdays and weekends.

	Command or Action	Purpose
	<p>Example:</p> <pre>SwitchController(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006</pre> <p>OR</p> <pre>SwitchController(config-time-range)# periodic weekdays 8:00 to 12:00</pre>	See the example configurations.
Step 5	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 6	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 7	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

What to Do Next

Repeat the steps if you have multiple items that you want in effect at different times.

Related Topics

[Time Ranges for ACLs, on page 168](#)

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line [console | vty] line-number**
4. **access-class access-list-number {in | out}**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController(config)# enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	line [console vty] line-number Example: SwitchController(config)# line console 0	Identifies a specific line to configure, and enter in-line configuration mode. <ul style="list-style-type: none"> • console—Specifies the console terminal line. The console port is DCE. • vty—Specifies a virtual terminal for remote console access. <p>The <i>line-number</i> is the first line number in a contiguous group that you want to configure when the line type is specified. The range is from 0 to 16.</p>
Step 4	access-class access-list-number {in out} Example: SwitchController(config-line)# access-class 10 in	Restricts incoming and outgoing connections between a particular virtual terminal line (into a device) and the addresses in an access list.
Step 5	end Example: SwitchController(config-line)# end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 7	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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:

SUMMARY STEPS

1. **configure terminal**
2. **interface *interface-id***
3. **ip access-group {*access-list-number* | *name*} {*in* | *out*}**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet1/0/1	Identifies a specific interface for configuration, and enter interface configuration mode. The interface can be a Layer 2 interface (port ACL), or a Layer 3 interface (router ACL).

	Command or Action	Purpose
Step 3	ip access-group { <i>access-list-number</i> <i>name</i> } { in out } Example: SwitchController(config-if)# ip access-group 2 in	Controls access to the specified interface. The out keyword is not supported for Layer 2 interfaces (port ACLs).
Step 4	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.
Step 5	show running-config Example: SwitchController# show running-config	Displays the access list configuration.
Step 6	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Related Topics

[IPv4 ACL Interface Considerations, on page 169](#)

[Restrictions for Configuring Network Security with ACLs, on page 154](#)

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mac access-list extended *name***
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** | **lavr-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp** | 0-65535] [**cos** *cos*]**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	mac access-list extended <i>name</i> Example: SwitchController (config) # mac access-list extended macl	Defines an extended MAC access list using a name.
Step 4	{deny permit} {any host <i>source MAC address</i> <i>source MAC address mask</i>} {any host <i>destination MAC address</i> <i>destination MAC address mask</i>} [<i>type mask</i> lsap <i>lsap mask</i> aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat lavr-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp 0-65535] [cos <i>cos</i>] Example: SwitchController (config-ext-macl) # deny any	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. (Optional) You can also enter these options: <ul style="list-style-type: none"> • <i>type mask</i>—An arbitrary EtherType number of a packet with Ethernet II or SNAP encapsulation in decimal, hexadecimal, or octal with optional mask of <i>don't care</i> bits applied to the EtherType before testing for a match.

	Command or Action	Purpose
	<pre>any decnet-iv</pre> <p>or</p> <pre>SwitchController(config-ext-macl)# permit any any</pre>	<ul style="list-style-type: none"> • lsap <i>lsap mask</i>—An LSAP number of a packet with IEEE 802.2 encapsulation in decimal, hexadecimal, or octal with optional mask of <i>don't care</i> 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 <i>cos</i>—An IEEE 802.1Q cost of service number from 0 to 7 used to set priority.
Step 5	<pre>end</pre> <p>Example:</p> <pre>SwitchController(config-ext-macl)# end</pre>	Returns to privileged EXEC mode.
Step 6	<pre>show running-config</pre> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 7	<pre>copy running-config startup-config</pre> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

[Restrictions for Configuring Network Security with ACLs, on page 154](#)

[Configuring VLAN Maps, on page 187](#)

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **mac access-group {*name*} {*in*}**
5. **end**
6. **show mac access-group [interface *interface-id*]**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet1/0/2	Identifies a specific interface, and enter interface configuration mode. The interface must be a physical Layer 2 interface (port ACL).
Step 4	mac access-group {<i>name</i>} {<i>in</i>} Example: SwitchController(config-if)# mac access-group mac1 in	Controls access to the specified interface by using the MAC access list. Port ACLs are supported in the inbound directions only.
Step 5	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	show mac access-group [interface <i>interface-id</i>] Example: SwitchController# show mac access-group interface gigabitethernet1/0/2	Displays the MAC access list applied to the interface or all Layer 2 interfaces.
Step 7	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 8	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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 Network Security with ACLs, on page 154](#)

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.

SUMMARY STEPS

1. **vlan access-map** *name* [**number**]
2. **match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*]
3. 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):

- **action** { **forward** }

```
SwitchController(config-access-map) # action forward
```

- **action** { **drop** }

```
SwitchController(config-access-map) # action drop
```

4. **vlan filter** *mapname* **vlan-list** *list*

DETAILED STEPS

	Command or Action	Purpose
Step 1	vlan access-map <i>name</i> [number] Example: <pre>SwitchController(config)# vlan access-map <i>map_1</i> 20</pre>	<p>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.</p> <p>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.</p> <p>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.</p> <p>Entering this command changes to access-map configuration mode.</p>
Step 2	match { ip mac } address { <i>name</i> <i>number</i> } [<i>name</i> <i>number</i>] Example: <pre>SwitchController(config-access-map)# match ip address <i>ip2</i></pre>	<p>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.</p> <p>Note If the VLAN map is configured with a match clause for a type of packet (IP or MAC) and the map action is drop, all packets that match the type are dropped. If the VLAN map has no match clause, and the configured action is drop, all IP and Layer 2 packets are dropped.</p>
Step 3	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):	Sets the action for the map entry.

	Command or Action	Purpose
	<ul style="list-style-type: none"> • action { forward} <pre>SwitchController(config-access-map)# action forward</pre> <ul style="list-style-type: none"> • action { drop} <pre>SwitchController(config-access-map)# action drop</pre>	
Step 4	<p>vlan filter <i>mapname</i> vlan-list <i>list</i></p> <p>Example:</p> <pre>SwitchController(config)# vlan filter map 1 vlan-list 20-22</pre>	<p>Applies the VLAN map to one or more VLAN IDs.</p> <p>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.</p>

Related Topics

- [Creating a Numbered Standard ACL, on page 170](#)
- [Creating a Numbered Extended ACL, on page 171](#)
- [Creating Named MAC Extended ACLs, on page 183](#)
- [Creating a VLAN Map, on page 189](#)
- [Applying a VLAN Map to a VLAN, on page 191](#)

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:

SUMMARY STEPS

1. **configure terminal**
2. **vlan access-map** *name* [**number**]
3. **match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*]
4. **action** {**drop** | **forward**}
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 2	vlan access-map name [number] Example: SwitchController (config)# vlan access-map map_1 20	<p>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.</p> <p>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.</p> <p>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.</p> <p>Entering this command changes to access-map configuration mode.</p>
Step 3	match {ip mac} address {name number} [name number] Example: SwitchController (config-access-map)# match ip address ip2	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.
Step 4	action {drop forward} Example: SwitchController (config-access-map)# action forward	(Optional) Sets the action for the map entry. The default is to forward.
Step 5	end Example: SwitchController (config-access-map)# end	Returns to global configuration mode.
Step 6	show running-config Example: SwitchController# show running-config	Displays the access list configuration.

	Command or Action	Purpose
Step 7	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

[Configuring VLAN Maps, on page 187](#)

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:

SUMMARY STEPS

1. **configure terminal**
2. **vlan filter *mapname* vlan-list *list***
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 2	vlan filter <i>mapname</i> vlan-list <i>list</i> Example: <pre>SwitchController(config)# vlan filter map 1 vlan-list 20-22</pre>	Applies the VLAN map to one or more VLAN IDs. 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.

	Command or Action	Purpose
Step 3	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.
Step 4	show running-config Example: SwitchController# show running-config	Displays the access list configuration.
Step 5	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Related Topics

[Configuring VLAN Maps, on page 187](#)

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 18: Commands for Displaying Access Lists and Access Groups

Command	Purpose
show access-lists [<i>number</i> <i>name</i>]	Displays the contents of one or all current IP and MAC address access lists or a specific access list (numbered or named).
show ip access-lists [<i>number</i> <i>name</i>]	Displays the contents of all current IP access lists or a specific IP access list (numbered or named).
show ip interface <i>interface-id</i>	Displays detailed configuration and status of an interface. If IP is enabled on the interface and ACLs have been applied by using the ip access-group interface configuration command, the access groups are included in the display.

Command	Purpose
show running-config [interface <i>interface-id</i>]	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.
show mac access-group [interface <i>interface-id</i>]	Displays MAC access lists applied to all Layer 2 interfaces or the specified Layer 2 interface.

You can also monitor VLAN maps by displaying information about VLAN access maps or VLAN filters. Use the privileged EXEC commands in this table to display VLAN map information.

Table 19: Commands for Displaying VLAN Map Information

Command	Purpose
show vlan access-map [<i>mapname</i>]	Displays information about all VLAN access maps or the specified access map.
show vlan filter [access-map <i>name</i> vlan <i>vlan-id</i>]	Displays information about all VLAN filters or about a specified VLAN or VLAN access map.

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.

```
SwitchController# show time-range
time-range entry: new_year_day_2006 (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.

```
SwitchController(config)# access-list 188 deny tcp any any time-range new_year_day_2006
SwitchController(config)# access-list 188 permit tcp any any time-range workhours
SwitchController(config)# end
SwitchController# 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.

```
SwitchController(config)# ip access-list extended deny_access
SwitchController(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
SwitchController(config-ext-nacl)# exit
SwitchController(config)# ip access-list extended may_access
SwitchController(config-ext-nacl)# permit tcp any any time-range workhours
SwitchController(config-ext-nacl)# end
SwitchController# show ip access-lists
Extended IP access list lpip_default
 10 permit ip any 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:

```
SwitchController(config)# access-list 1 remark Permit only Jones workstation through
SwitchController(config)# access-list 1 permit 171.69.2.88
SwitchController(config)# access-list 1 remark Do not allow Smith through
SwitchController(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:

```
SwitchController(config)# ip access-list extended telnetting
SwitchController(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
SwitchController(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

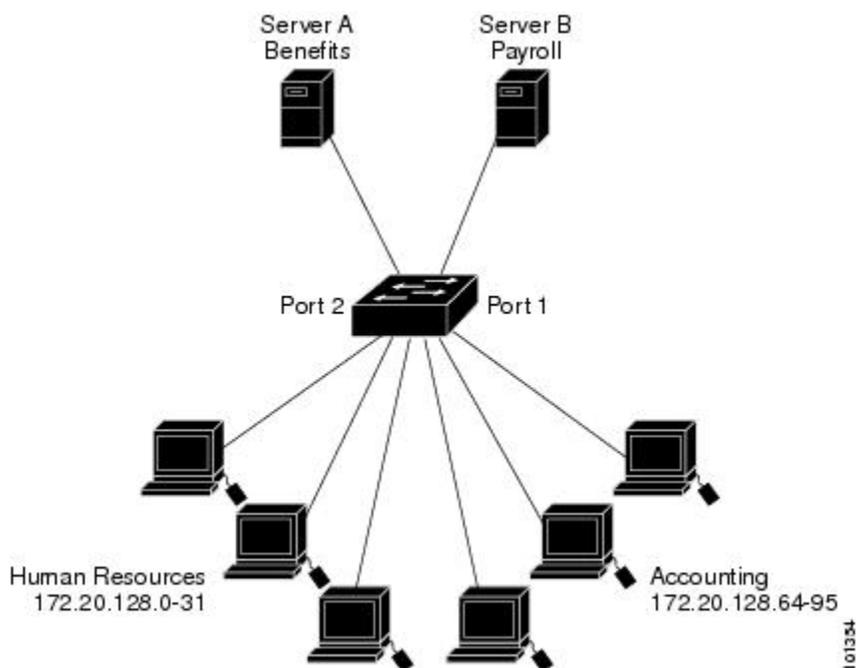
IPv4 ACL Configuration Examples

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

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.

Figure 5: Using Router ACLs to Control Traffic



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.

```
SwitchController(config)# access-list 6 permit 172.20.128.64 0.0.0.31
SwitchController(config)# end
SwitchController# show access-lists
Standard IP access list 6
 10 permit 172.20.128.64, wildcard bits 0.0.0.31
SwitchController(config)# interface gigabitethernet1/0/1
SwitchController(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.

```
SwitchController(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
SwitchController(config)# end
SwitchController# show access-lists
Extended IP access list 106
  10 permit ip any 172.20.128.64 0.0.0.31
SwitchController(config)# interface gigabitethernet1/0/1
SwitchController(config-if)# ip access-group 106 in
```

Example: Numbered ACLs

In this example, network 36.0.0.0 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 36.0.0.0 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 36.0.0.0 subnets. The ACL is applied to packets entering a port.

```
SwitchController(config)# access-list 2 permit 36.48.0.3
SwitchController(config)# access-list 2 deny 36.48.0.0 0.0.255.255
SwitchController(config)# access-list 2 permit 36.0.0.0 0.255.255.255
SwitchController(config)# interface gigabitethernet2/0/1
SwitchController(config-if)# ip access-group 2 in
```

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.

```
SwitchController(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
SwitchController(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
SwitchController(config)# access-list 102 permit icmp any any
SwitchController(config)# interface gigabitethernet2/0/1
SwitchController(config-if)# ip access-group 102 in
```

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.

```
SwitchController(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
SwitchController(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
SwitchController(config)# interface gigabitethernet1/0/1
SwitchController(config-if)# ip access-group 102 in
```

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.

```
SwitchController(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
SwitchController(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
SwitchController(config)# interface gigabitethernet1/0/1
SwitchController(config-if)# ip access-group 102 in
```

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.

```
SwitchController(config)# ip access-list standard Internet_filter
SwitchController(config-ext-nacl)# permit 1.2.3.4
SwitchController(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.

```
SwitchController(config)# ip access-list extended marketing_group
SwitchController(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
SwitchController(config-ext-nacl)# deny tcp any any
SwitchController(config-ext-nacl)# permit icmp any any
SwitchController(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
SwitchController(config-ext-nacl)# deny ip any any log
SwitchController(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.

```
SwitchController(config)# interface gigabitethernet3/0/2
SwitchController(config-if)# no switchport
SwitchController(config-if)# ip address 2.0.5.1 255.255.255.0
SwitchController(config-if)# ip access-group Internet_filter out
SwitchController(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*:

```
SwitchController(config)# ip access-list extended border-list
SwitchController(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).

```
SwitchController(config)# time-range no-http
SwitchController(config)# periodic weekdays 8:00 to 18:00
!
SwitchController(config)# time-range udp-yes
SwitchController(config)# periodic weekend 12:00 to 20:00
!
SwitchController(config)# ip access-list extended strict
SwitchController(config-ext-nacl)# deny tcp any any eq www time-range no-http
SwitchController(config-ext-nacl)# permit udp any any time-range udp-yes
!
SwitchController(config-ext-nacl)# exit
SwitchController(config)# interface gigabitethernet2/0/1
SwitchController(config-if)# ip access-group strict in
```

Examples: 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:

```
SwitchController(config)# access-list 1 remark Permit only Jones workstation through
SwitchController(config)# access-list 1 permit 171.69.2.88
SwitchController(config)# access-list 1 remark Do not allow Smith workstation through
SwitchController(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:

```
SwitchController(config)# access-list 100 remark Do not allow Winter to browse the web
SwitchController(config)# access-list 100 deny host 171.69.3.85 any eq www
SwitchController(config)# access-list 100 remark Do not allow Smith to browse the web
SwitchController(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:

```
SwitchController(config)# ip access-list standard prevention
SwitchController(config-std-nacl)# remark Do not allow Jones subnet through
SwitchController(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:

```
SwitchController(config)# ip access-list extended telnetting
SwitchController(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
SwitchController(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 *stan1* denies traffic from 10.1.1.0 0.0.0.255, allows traffic from all other sources, and includes the **log** keyword.

```
SwitchController(config)# ip access-list standard stan1
SwitchController(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
SwitchController(config-std-nacl)# permit any log
SwitchController(config-std-nacl)# exit
SwitchController(config)# interface gigabitethernet1/0/1
SwitchController(config-if)# ip access-group stan1 in
SwitchController(config-if)# end
SwitchController# 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.

```
SwitchController(config)# ip access-list extended ext1
SwitchController(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
SwitchController(config-ext-nacl)# deny udp any any log
SwitchController(config-ext-nacl)# exit
SwitchController(config)# interface gigabitethernet1/0/2
SwitchController(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 (0/0), 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-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1 packet
01:31:33:%SEC-6-IPACCESSLOGP: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:

```
00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0), 1
packet
```

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.

```
SwitchController(config)# ip access-list extended ip1
SwitchController(config-ext-nacl)# permit tcp any any
SwitchController(config-ext-nacl)# exit
SwitchController(config)# vlan access-map map_1 10
SwitchController(config-access-map)# match ip address ip1
SwitchController(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.

```
SwitchController(config)# ip access-list extended ip2
SwitchController(config-ext-nacl)# permit udp any any
SwitchController(config-ext-nacl)# exit
SwitchController(config)# vlan access-map map_1 20
SwitchController(config-access-map)# match ip address ip2
SwitchController(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

```
SwitchController(config)# access-list 101 permit udp any any
SwitchController(config)# ip access-list extended igmp-match
SwitchController(config-ext-nacl)# permit igmp any any
SwitchController(config)# ip access-list extended tcp-match

SwitchController(config-ext-nacl)# permit tcp any any
SwitchController(config-ext-nacl)# exit
SwitchController(config)# vlan access-map drop-ip-default 10
SwitchController(config-access-map)# match ip address 101
SwitchController(config-access-map)# action forward
```

```
SwitchController(config-access-map) # exit
SwitchController(config) # vlan access-map drop-ip-default 20
SwitchController(config-access-map) # match ip address igmp-match
SwitchController(config-access-map) # action drop
SwitchController(config-access-map) # exit
SwitchController(config) # vlan access-map drop-ip-default 30
SwitchController(config-access-map) # match ip address tcp-match
SwitchController(config-access-map) # 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

```
SwitchController(config) # mac access-list extended good-hosts
SwitchController(config-ext-macl) # permit host 000.0c00.0111 any
SwitchController(config-ext-macl) # permit host 000.0c00.0211 any
SwitchController(config-ext-nacl) # exit
SwitchController(config) # mac access-list extended good-protocols
SwitchController(config-ext-macl) # permit any any decnet-ip
SwitchController(config-ext-macl) # permit any any vines-ip
SwitchController(config-ext-nacl) # exit
SwitchController(config) # vlan access-map drop-mac-default 10
SwitchController(config-access-map) # match mac address good-hosts
SwitchController(config-access-map) # action forward
SwitchController(config-access-map) # exit
SwitchController(config) # vlan access-map drop-mac-default 20
SwitchController(config-access-map) # match mac address good-protocols
SwitchController(config-access-map) # action forward
```

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

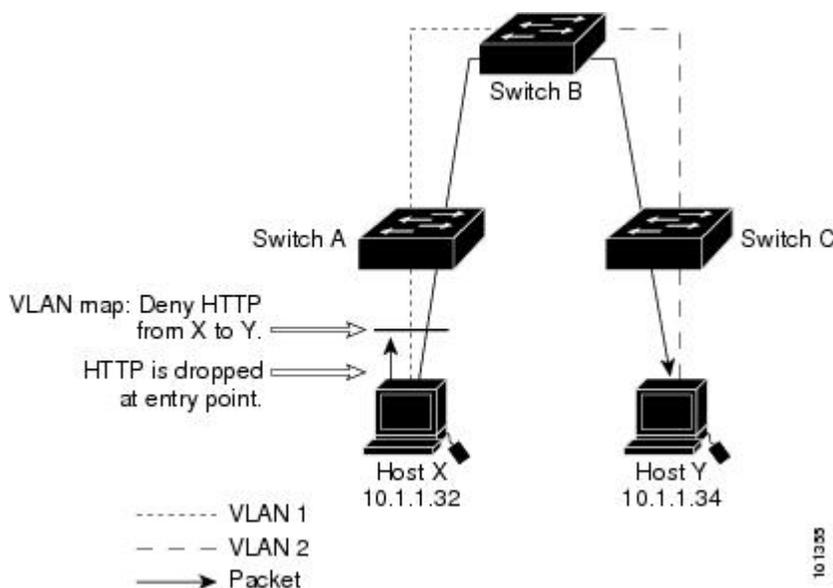
```
SwitchController(config) # vlan access-map drop-all-default 10
SwitchController(config-access-map) # match ip address tcp-match
SwitchController(config-access-map) # action forward
SwitchController(config-access-map) # exit
SwitchController(config) # vlan access-map drop-all-default 20
SwitchController(config-access-map) # match mac address good-hosts
SwitchController(config-access-map) # action forward
```

Configuration Examples for Using VLAN Maps in Your Network

Example: 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.

Figure 6: Wiring Closet Configuration



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.

```
SwitchController(config)# ip access-list extended http
SwitchController(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
SwitchController(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.

```
SwitchController(config)# vlan access-map map2 10
SwitchController(config-access-map)# match ip address http
SwitchController(config-access-map)# action drop
SwitchController(config-access-map)# exit
SwitchController(config)# ip access-list extended match_all
SwitchController(config-ext-nacl)# permit ip any any
SwitchController(config-ext-nacl)# exit
SwitchController(config)# vlan access-map map2 20
```

```
SwitchController(config-access-map)# match ip address match_all
SwitchController(config-access-map)# action forward
```

Then, apply VLAN access map *map2* to VLAN 1.

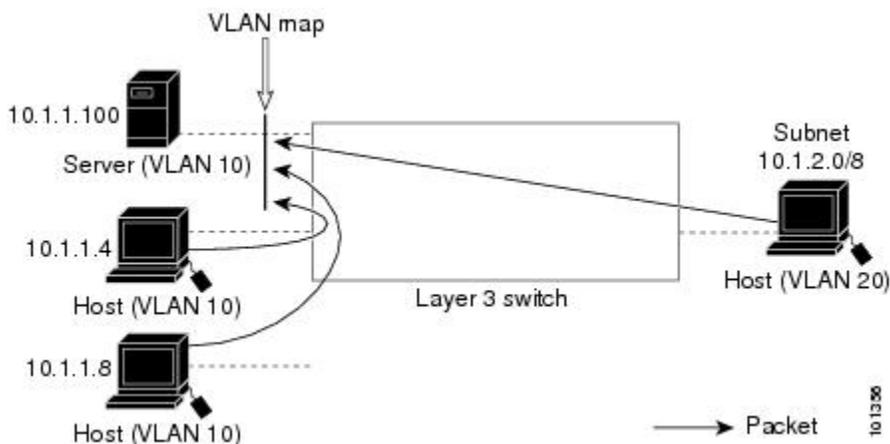
```
SwitchController(config)# vlan filter map2 vlan 1
```

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.

Figure 7: Restricting Access to a Server on Another VLAN



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.

```
SwitchController(config)# ip access-list extended SERVER1_ACL
SwitchController(config-ext-nacl)# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
SwitchController(config-ext-nacl)# permit ip host 10.1.1.4 host 10.1.1.100
SwitchController(config-ext-nacl)# permit ip host 10.1.1.8 host 10.1.1.100
SwitchController(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.

```
SwitchController(config)# vlan access-map SERVER1_MAP
SwitchController(config-access-map)# match ip address SERVER1_ACL
SwitchController(config-access-map)# action drop
```

```
SwitchController(config)# vlan access-map SERVER1_MAP 20
SwitchController(config-access-map)# action forward
SwitchController(config-access-map)# exit
```

Apply the VLAN map to VLAN 10.

```
SwitchController(config)# vlan filter SERVER1_MAP vlan-list 10
```

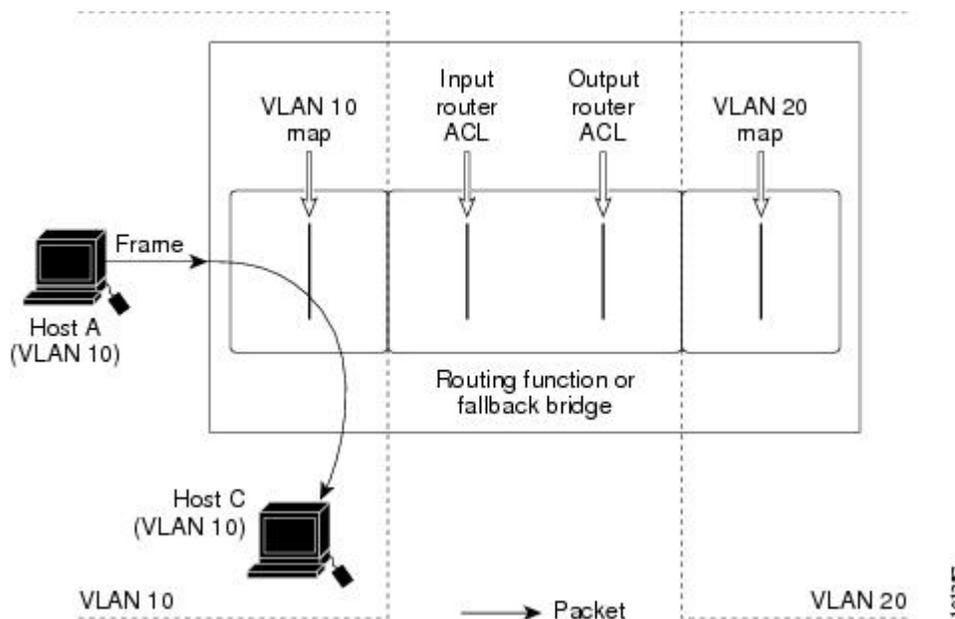
Configuration Examples of Router ACLs and VLAN Maps Applied to VLANs

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

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.

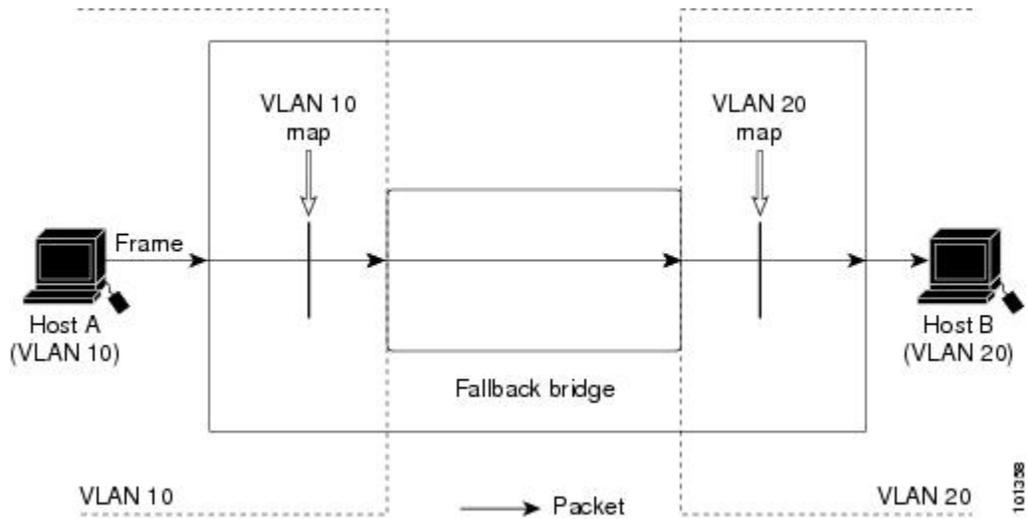
Figure 8: Applying ACLs on Switched Packets



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.

Figure 9: Applying ACLs on Bridged Packets

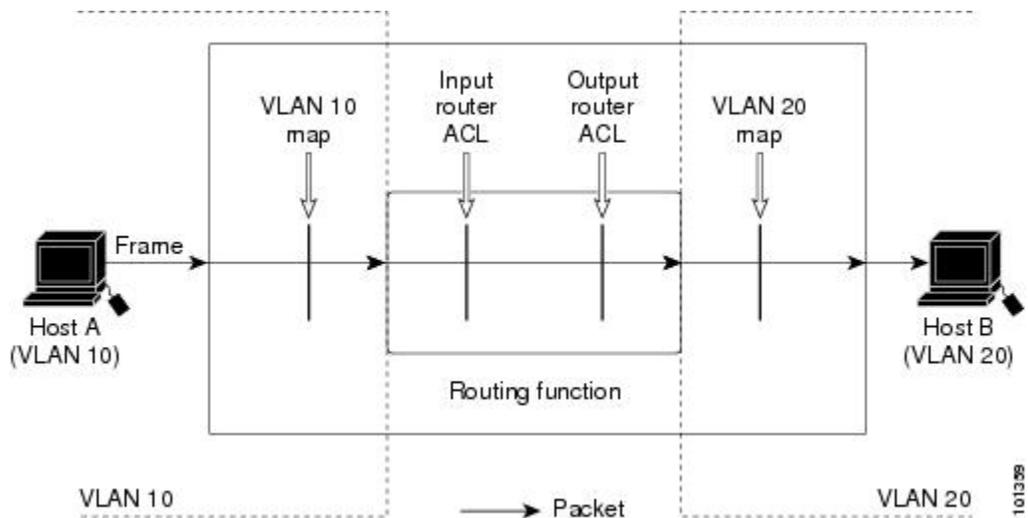


Example: ACLs and Routed Packets

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

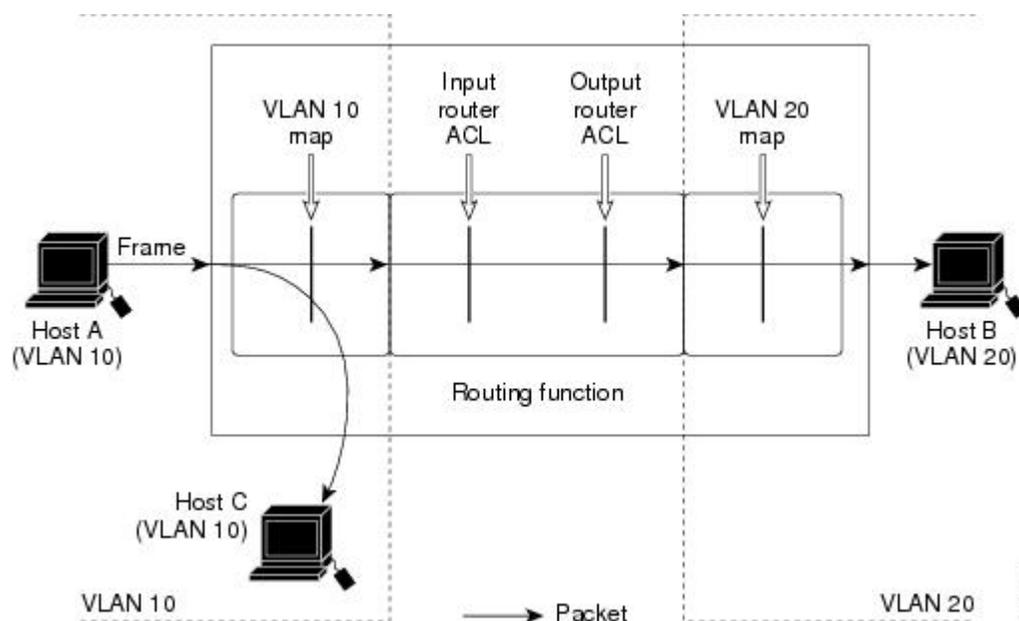
Figure 10: Applying ACLs on Routed Packets



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.

Figure 11: Applying ACLs on Multicast Packets



Additional References

Related Documents

Related Topic	Document Title
IPv4 Access Control List topics	Securing the Data Plane Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secdata-xe-3se-3850-library.html

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

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support



CHAPTER 13

Configuring DHCP

- [Finding Feature Information, page 209](#)
- [Information About DHCP, page 209](#)
- [How to Configure DHCP Features, page 216](#)
- [Configuring DHCP Server Port-Based Address Allocation, page 228](#)

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 DHCP OFFER, DHCP ACK, DHCP NAK, or DHCP REQUEST 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 DHCP RELEASE or DHCP DECLINE 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.

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.

Related Topics

[Prerequisites for Configuring DHCP Snooping and Option 82, on page 222](#)

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.



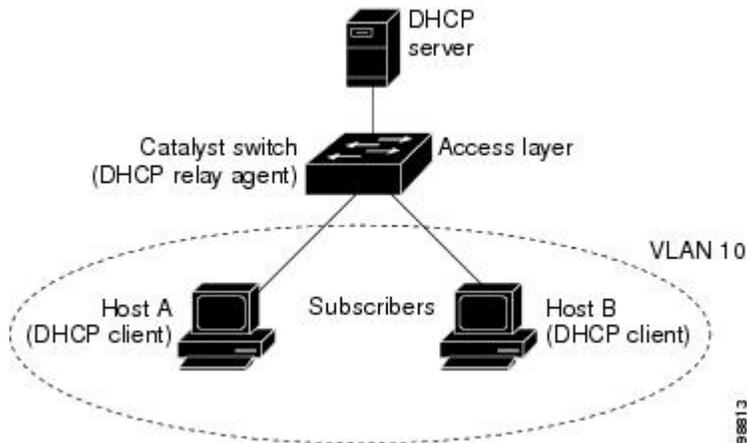
Note

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.

Figure 12: DHCP Relay Agent in a Metropolitan Ethernet Network



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

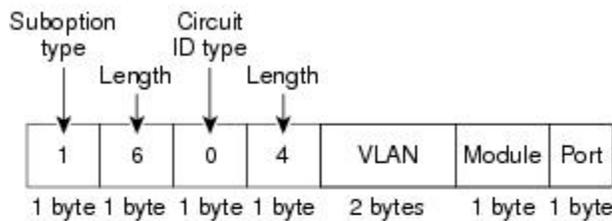
- Remote-ID suboption fields
 - Suboption type
 - Length of the suboption type
 - Remote-ID type
 - Length of the remote-ID type

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`.

Figure 13: Suboption Packet Formats

Circuit ID Suboption Frame Format



Remote ID Suboption Frame Format



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.

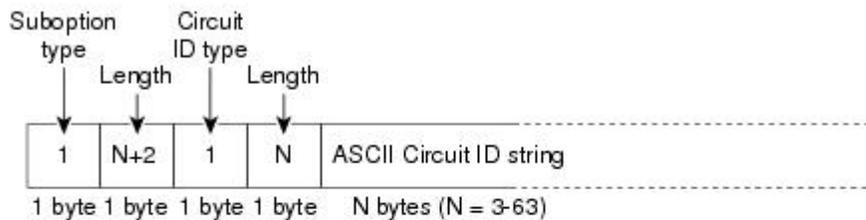
The values for these fields in the packets change from the default values when you configure the remote-ID and circuit-ID suboptions:

- Circuit-ID suboption fields
 - The circuit-ID type is 1.

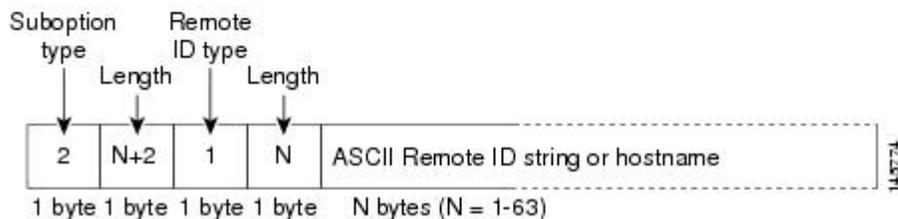
- The length values are variable, depending on the length of the string that you configure.
- Remote-ID suboption fields
 - The remote-ID type is 1.
 - The length values are variable, depending on the length of the string that you configure.

Figure 14: User-Configured Suboption Packet Formats

Circuit ID Suboption Frame Format (for user-configured string):



Remote ID Suboption Frame Format (for user-configured string):



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 20: Default DHCP Configuration

Feature	Default Setting
DHCP server	Enabled in Cisco IOS software, requires configuration ⁶
DHCP relay agent	Enabled ⁷
DHCP packet forwarding address	None configured
Checking the relay agent information	Enabled (invalid messages are dropped)
DHCP relay agent forwarding policy	Replace the existing relay agent information
DHCP snooping enabled globally	Disabled
DHCP snooping information option	Enabled
DHCP snooping option to accept packets on untrusted input interfaces ⁸	Disabled
DHCP snooping limit rate	None configured
DHCP snooping trust	Untrusted
DHCP snooping VLAN	Disabled
DHCP snooping MAC address verification	Enabled

Feature	Default Setting
Cisco IOS DHCP server binding database	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.
DHCP snooping binding database agent	Enabled in Cisco IOS software, requires configuration. This feature is operational only when a destination is configured.

⁶ The switch responds to DHCP requests only if it is configured as a DHCP server.

⁷ The switch relays DHCP packets only if the IP address of the DHCP server is configured on the SVI of the DHCP client.

⁸ Use this feature when the switch is an aggregation switch that receives packets with option-82 information from an edge switch.

DHCP Snooping Configuration Guidelines

- DHCP snooping is not active until DHCP snooping is enabled on a VLAN.
- When configuring a large number of circuit IDs on a switch, consider the impact of lengthy character strings on the NVRAM or the flash memory. If the circuit-ID configurations, combined with other data, exceed the capacity of the NVRAM or the flash memory, an error message appears.
- If the DHCP relay agent is enabled but DHCP snooping is disabled, the DHCP option-82 data insertion feature is not supported.
- 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. 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.

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. If the stack master fails, all unsaved bindings are lost. 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.

When a stack merge occurs, the stack master that becomes a stack member loses all of the DHCP lease bindings. With a stack partition, the new master in the partition acts as a new DHCP server without any of the existing DHCP lease bindings.

Configuring the DHCP Relay Agent

Follow these steps to enable the DHCP relay agent on the switch:

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `service dhcp`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example:</p> <pre>SwitchController> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p><code>service dhcp</code></p> <p>Example:</p> <pre>SwitchController(config)# service dhcp</pre>	Enables the DHCP server and relay agent on your switch. By default, this feature is enabled.
Step 4	<p><code>end</code></p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 6	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

What to Do Next

See the “*Configuring DHCP*” section of the “IP Addressing and Services” section of the *Cisco IOS IP Configuration Guide, Release 12.4* for these procedures:

- 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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vlan** *vlan-id*
4. **ip address** *ip-address subnet-mask*
5. **ip helper-address** *address*
6. **end**
7. Use one of the following:
 - **interface range** *port-range*
 - **interface** *interface-id*
8. **switchport mode access**
9. **switchport access vlan** *vlan-id*
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	interface vlan <i>vlan-id</i> Example: SwitchController(config)# interface vlan 1	Creates a switch virtual interface by entering a VLAN ID, and enter interface configuration mode.
Step 4	ip address <i>ip-address subnet-mask</i> Example: SwitchController(config-if)# ip address 192.108.1.27 255.255.255.0	Configures the interface with an IP address and an IP subnet.
Step 5	ip helper-address <i>address</i>	Specifies the DHCP packet forwarding address.

	Command or Action	Purpose
	<p>Example:</p> <pre>SwitchController(config-if)# ip helper-address 172.16.1.2</pre>	<p>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.</p> <p>If you have multiple servers, you can configure one helper address for each server.</p>
Step 6	<p>end</p> <p>Example:</p> <pre>SwitchController(config-if)# end</pre>	Returns to global configuration mode.
Step 7	<p>Use one of the following:</p> <ul style="list-style-type: none"> • interface range <i>port-range</i> • interface <i>interface-id</i> <p>Example:</p> <pre>SwitchController(config)# interface gigabitethernet1/0/2</pre>	<p>Configures multiple physical ports that are connected to the DHCP clients, and enter interface range configuration mode.</p> <p>or</p> <p>Configures a single physical port that is connected to the DHCP client, and enter interface configuration mode.</p>
Step 8	<p>switchport mode access</p> <p>Example:</p> <pre>SwitchController(config-if)# switchport mode access</pre>	Defines the VLAN membership mode for the port.
Step 9	<p>switchport access vlan <i>vlan-id</i></p> <p>Example:</p> <pre>SwitchController(config-if)# switchport access vlan 1</pre>	Assigns the ports to the same VLAN as configured in Step 2.
Step 10	<p>end</p> <p>Example:</p> <pre>SwitchController(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 11	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.

	Command or Action	Purpose
Step 12	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

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.
- DHCP snooping is not active until DHCP snooping is enabled on a VLAN.
- 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:
 - 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.
- When you configure DHCP snooping smart logging, the contents of packets dropped by DHCP are sent to a NetFlow collector. If you configure this feature, make sure that smart logging is globally enabled.



Note Do not enable Dynamic Host Configuration Protocol (DHCP) snooping on RSPAN VLANs. If DHCP snooping is enabled on RSPAN VLANs, DHCP packets might not reach the RSPAN destination port.

- When configuring a large number of circuit IDs on a switch, consider the impact of lengthy character strings on the NVRAM or the flash memory. If the circuit-ID configurations, combined with other data, exceed the capacity of the NVRAM or the flash memory, an error message appears.
- 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 the DHCP relay agent is enabled but DHCP snooping is disabled, the DHCP option-82 data insertion feature is not supported.
- 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.
- Do not enter the **ip dhcp snooping information option allow-untrusted** command on an aggregation switch to which an untrusted device is connected. If you enter this command, an untrusted device might spoof the option-82 information.

Related Topics

[DHCP Snooping, on page 210](#)

Enabling DHCP Snooping and Option 82

Follow these steps to enable DHCP snooping on the switch:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp snooping**
4. **ip dhcp snooping vlan *vlan-range* [smartlog]**
5. **ip dhcp snooping information option**
6. **ip dhcp snooping information option format remote-id [string *ASCII-string* | hostname]**
7. **ip dhcp snooping information option allow-untrusted**
8. **ip dhcp snooping wireless bootp-broadcast enable (optional)**
9. **interface *interface-id***
10. **ip dhcp snooping vlan *vlan* information option format-type circuit-id [override] string *ASCII-string***
11. **ip dhcp snooping trust**
12. **ip dhcp snooping limit rate *rate***
13. **exit**
14. **ip dhcp snooping verify mac-address**
15. **end**
16. **show running-config**
17. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	ip dhcp snooping Example: SwitchController(config)# ip dhcp snooping	Enables DHCP snooping globally.

	Command or Action	Purpose
Step 4	<p>ip dhcp snooping vlan <i>vlan-range</i> [smartlog]</p> <p>Example:</p> <pre>SwitchController(config)# ip dhcp snooping vlan 10</pre>	<p>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.</p> <ul style="list-style-type: none"> 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. (Optional) Enter smartlog to configure the switch to send the contents of dropped packets to a NetFlow collector.
Step 5	<p>ip dhcp snooping information option</p> <p>Example:</p> <pre>SwitchController(config)# ip dhcp snooping information option</pre>	<p>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.</p>
Step 6	<p>ip dhcp snooping information option format remote-id [<i>string ASCII-string</i> <i>hostname</i>]</p> <p>Example:</p> <pre>SwitchController(config)# ip dhcp snooping information option format remote-id string acsiistring2</pre>	<p>(Optional) Configures the remote-ID suboption.</p> <p>You can configure the remote ID as:</p> <ul style="list-style-type: none"> String of up to 63 ASCII characters (no spaces) Configured hostname for the switch <p>Note If the hostname is longer than 63 characters, it is truncated to 63 characters in the remote-ID configuration.</p> <p>The default remote ID is the switch MAC address.</p>
Step 7	<p>ip dhcp snooping information option allow-untrusted</p> <p>Example:</p> <pre>SwitchController(config)# ip dhcp snooping information option allow-untrusted</pre>	<p>(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.</p> <p>The default setting is disabled.</p> <p>Note Enter this command only on aggregation switches that are connected to trusted devices.</p>
Step 8	<p>ip dhcp snooping wireless bootp-broadcast enable (optional)</p> <p>Example:</p> <pre>SwitchController(config)# ip dhcp snooping wireless bootp-broadcast enable</pre>	<p>Enables broadcast address sent by the server to be retained by the switch when it forwards DHCP packets to wireless clients.</p>

	Command or Action	Purpose
Step 9	<p>interface <i>interface-id</i></p> <p>Example:</p> <pre>SwitchController(config)# interface gigabitethernet2/0/1</pre>	Specifies the interface to be configured, and enter interface configuration mode.
Step 10	<p>ip dhcp snooping vlan <i>vlan</i> information option format-type circuit-id [override] string <i>ASCII-string</i></p> <p>Example:</p> <pre>SwitchController(config-if)# ip dhcp snooping vlan 1 information option format-type circuit-id override string ovrride2</pre>	<p>(Optional) Configures the circuit-ID suboption for the specified interface.</p> <p>Specify the VLAN and port identifier, using a VLAN ID in the range of 1 to 4094. The default circuit ID is the port identifier, in the format vlan-mod-port.</p> <p>You can configure the circuit ID to be a string of 3 to 63 ASCII characters (no spaces).</p> <p>(Optional) Use the override keyword when you do not want the circuit-ID suboption inserted in TLV format to define subscriber information.</p>
Step 11	<p>ip dhcp snooping trust</p> <p>Example:</p> <pre>SwitchController(config-if)# ip dhcp snooping trust</pre>	(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.
Step 12	<p>ip dhcp snooping limit rate <i>rate</i></p> <p>Example:</p> <pre>SwitchController(config-if)# ip dhcp snooping limit rate 100</pre>	<p>(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.</p> <p>Note 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.</p>
Step 13	<p>exit</p> <p>Example:</p> <pre>SwitchController(config-if)# exit</pre>	Returns to global configuration mode.
Step 14	<p>ip dhcp snooping verify mac-address</p> <p>Example:</p> <pre>SwitchController(config)# ip dhcp snooping verify mac-address</pre>	(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.

	Command or Action	Purpose
Step 15	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.
Step 16	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 17	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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 21: Commands for Displaying DHCP Information

show ip dhcp snooping	Displays the DHCP snooping configuration for a switch
show ip dhcp snooping binding	Displays only the dynamically configured bindings in the DHCP snooping binding database, also referred to as a binding table.
show ip dhcp snooping database	Displays the DHCP snooping binding database status and statistics.
show ip dhcp snooping statistics	Displays the DHCP snooping statistics in summary or detail form.
show ip source binding	Display the dynamically and statically configured bindings.

**Note**

If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

Configuring DHCP Server Port-Based Address Allocation

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.
- Only one IP address can be assigned per port.
- Reserved addresses (preassigned) cannot be cleared by using the `clear ip dhcp binding` global configuration command.
- Preassigned addresses are automatically excluded from normal dynamic IP address assignment. Preassigned addresses cannot be used in host pools, but there can be multiple preassigned addresses per DHCP address pool.

- 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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp snooping database** {flash[number]:/filename | ftp://user:password@host/filename | http://[[username:password]@]{hostname | host-ip}[/directory] /image-name.tar | rcp://user@host/filename} | tftp://host/filename
4. **ip dhcp snooping database timeout** seconds
5. **ip dhcp snooping database write-delay** seconds
6. **end**
7. **ip dhcp snooping binding** mac-address vlan vlan-id ip-address **interface** interface-id **expiry** seconds
8. **show ip dhcp snooping database** [detail]
9. **show running-config**
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	ip dhcp snooping database {flash[number]:/filename ftp://user:password@host/filename http://[[username:password]@]{hostname host-ip}[/directory] /image-name.tar rcp://user@host/filename} tftp://host/filename	Specifies the URL for the database agent or the binding file by using one of these forms: <ul style="list-style-type: none"> • flash[number]:/filename (Optional) Use the <i>number</i> parameter to specify the stack member number of the stack master. The range for <i>number</i> is 1 to 9.

	Command or Action	Purpose
	<p>Example:</p> <pre>SwitchController(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2</pre>	<ul style="list-style-type: none"> • <code>ftp://user:password@host/filename</code> • <code>http://[[username:password]@]{hostname host-ip}{/directory} /image-name.tar</code> • <code>rcp://user@host/filename</code> • <code>tftp://host/filename</code>
Step 4	<p>ip dhcp snooping database timeout <i>seconds</i></p> <p>Example:</p> <pre>SwitchController(config)# ip dhcp snooping database timeout 300</pre>	<p>Specifies (in seconds) how long to wait for the database transfer process to finish before stopping the process.</p> <p>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.</p>
Step 5	<p>ip dhcp snooping database write-delay <i>seconds</i></p> <p>Example:</p> <pre>SwitchController(config)# ip dhcp snooping database write-delay 15</pre>	<p>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).</p>
Step 6	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	<p>Returns to privileged EXEC mode.</p>
Step 7	<p>ip dhcp snooping binding <i>mac-address</i> vlan <i>vlan-id</i> <i>ip-address</i> interface <i>interface-id</i> expiry <i>seconds</i></p> <p>Example:</p> <pre>SwitchController# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000</pre>	<p>(Optional) Adds binding entries to the DHCP snooping binding database. The <i>vlan-id</i> range is from 1 to 4904. The <i>seconds</i> range is from 1 to 4294967295.</p> <p>Enter this command for each entry that you add.</p> <p>Use this command when you are testing or debugging the switch.</p>
Step 8	<p>show ip dhcp snooping database [detail]</p> <p>Example:</p> <pre>SwitchController# show ip dhcp snooping database detail</pre>	<p>Displays the status and statistics of the DHCP snooping binding database agent.</p>
Step 9	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	<p>Verifies your entries.</p>

	Command or Action	Purpose
Step 10	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp use subscriber-id client-id**
4. **ip dhcp subscriber-id interface-name**
5. **interface *interface-id***
6. **ip dhcp server use subscriber-id client-id**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>SwitchController> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	ip dhcp use subscriber-id client-id Example: <pre>SwitchController(config)# ip dhcp use subscriber-id client-id</pre>	Configures the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.
Step 4	ip dhcp subscriber-id interface-name Example: <pre>SwitchController(config)# ip dhcp subscriber-id interface-name</pre>	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.
Step 5	interface interface-id Example: <pre>SwitchController(config)# interface gigabitethernet1/0/1</pre>	Specifies the interface to be configured, and enter interface configuration mode.
Step 6	ip dhcp server use subscriber-id client-id Example: <pre>SwitchController(config-if)# ip dhcp server use subscriber-id client-id</pre>	Configures the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on the interface.
Step 7	end Example: <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 8	show running-config Example: <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 9	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

What to Do Next

After enabling DHCP port-based address allocation on the switch, use the **ip dhcp pool** global configuration command to preassign IP addresses and to associate them to clients.

Monitoring DHCP Server Port-Based Address Allocation

Table 22: Commands for Displaying DHCP Port-Based Address Allocation Information

Command	Purpose
show interface <i>interface id</i>	Displays the status and configuration of a specific interface.
show ip dhcp pool	Displays the DHCP address pools.
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.

Additional References

Related Documents

Related Topic	Document Title
DHCP Configuration Information and Procedures	IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 3S http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/dhcp-xe-3s-book.html

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

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/support</p>



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, page 235](#)
- [Information About IP Source Guard, page 235](#)
- [How to Configure IP Source Guard, page 238](#)
- [Monitoring IP Source Guard, page 242](#)
- [Additional References, page 242](#)

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.

- If you enable IP source guard with source IP and MAC address filtering, DHCP snooping and port security must be enabled on the interface. You must also enter the **ip dhcp snooping information option** global configuration command and ensure that the DHCP server supports option 82. When IP source guard is enabled with MAC address filtering, the DHCP host MAC address is not learned until the host is granted a lease. When forwarding packets from the server to the host, DHCP snooping uses option-82 data to identify the host port.
- When configuring IP source guard on interfaces on which a private VLAN is configured, port security is not supported.
- You can enable this feature when 802.1x port-based authentication is enabled.
- If the number of ternary content addressable memory (TCAM) entries exceeds the maximum, the CPU usage increases.
- 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 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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip verify source** [**mac-check**]
5. Use one of the following:
 - **ip verify source**[**smartlog**]
 - **ip verify source port-security**
6. **exit**
7. **ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet 1/0/1	Specifies the interface to be configured, and enters interface configuration mode.
Step 4	ip verify source [mac-check]	Enables IP source guard with source IP address filtering.

	Command or Action	Purpose
	<p>Example: SwitchController(config-if) # ip verify source</p>	(Optional) mac-check —Enables IP Source Guard with source IP address and MAC address filtering.
Step 5	<p>Use one of the following:</p> <ul style="list-style-type: none"> • ip verify source[smartlog] • ip verify source port-security <p>Example: SwitchController(config-if) # ip verify source</p> <p>or</p> <p>SwitchController(config-if) # ip verify source port-security</p>	<p>Enables IP source guard with source IP address filtering.</p> <p>(Optional) Enter smartlog to configure the switch to send the contents of dropped packets to a NetFlow collector.</p> <p>Enables IP source guard with source IP and MAC address filtering.</p> <p>When you enable both IP source guard and port security by using the ip verify source port-security interface configuration command, there are two caveats:</p> <ul style="list-style-type: none"> • The DHCP server must support option 82, or the client is not assigned an IP address. • The MAC address in the DHCP packet is not learned as a secure address. The MAC address of the DHCP client is learned as a secure address only when the switch receives non-DHCP data traffic.
Step 6	<p>exit</p> <p>Example: SwitchController(config-if) # exit</p>	Returns to global configuration mode.
Step 7	<p>ip source binding mac-address vlan vlan-id ip-address interface interface-id</p> <p>Example: SwitchController(config) # ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1</p>	<p>Adds a static IP source binding.</p> <p>Enter this command for each static binding.</p>
Step 8	<p>end</p> <p>Example: SwitchController(config) # end</p>	Returns to privileged EXEC mode.
Step 9	<p>show running-config</p> <p>Example: SwitchController# show running-config</p>	Verifies your entries.

	Command or Action	Purpose
Step 10	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

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. This requirement also applies to IPSG with static hosts on a private VLAN host port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip device tracking**
4. **interface *interface-id***
5. **switchport mode access**
6. **switchport access vlan *vlan-id***
7. **ip verify source[tracking] [mac-check]**
8. **ip device tracking maximum *number***
9. **switchport port-security**
10. **switchport port-security maximum *value***
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>SwitchController> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	ip device tracking Example: SwitchController(config)# ip device tracking	Turns on the IP host table, and globally enables IP device tracking.
Step 4	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet 1/0/1	Enters interface configuration mode.
Step 5	switchport mode access Example: SwitchController(config-if)# switchport mode access	Configures a port as access.
Step 6	switchport access vlan <i>vlan-id</i> Example: SwitchController(config-if)# switchport access vlan 10	Configures the VLAN for this port.
Step 7	ip verify source[tracking] [mac-check] Example: SwitchController(config-if)# ip verify source tracking mac-check	<p>Enables IP source guard with source IP address filtering.</p> <p>(Optional) tracking—Enables IP source guard for static hosts.</p> <p>(Optional) mac-check—Enables MAC address filtering.</p> <p>The command ip verify source tracking mac-check enables IP source guard for static hosts with MAC address filtering.</p>
Step 8	ip device tracking maximum <i>number</i> Example: SwitchController(config-if)# ip device tracking maximum 8	<p>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.</p> <p>Note You must configure the ip device tracking maximum <i>limit-number</i> interface configuration command.</p>
Step 9	switchport port-security	(Optional) Activate port security for this port.

	Command or Action	Purpose
Step 10	<code>switchport port-security maximum <i>value</i></code>	(Optional) Establish a maximum of MAC addresses for this port.
Step 11	end Example: <code>SwitchController(config)# end</code>	Returns to privileged EXEC mode.

Monitoring IP Source Guard

Table 23: Privileged EXEC show Commands

Command	Purpose
<code>show ip verify source [interface <i>interface-id</i>]</code>	Displays the IP source guard configuration on the switch or on a specific interface.
<code>show ip device tracking { all interface <i>interface-id</i> ip <i>ip-address</i> mac <i>mac-address</i> }</code>	Displays information about the entries in the IP device tracking table.

Table 24: Interface Configuration Commands

Command	Purpose
<code>ip verify source tracking</code>	Verifies the data source.

For detailed information about the fields in these displays, see the command reference for this release.

Additional References

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

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support



Configuring Dynamic ARP Inspection

- [Finding Feature Information, page 245](#)
- [Restrictions for Dynamic ARP Inspection, page 245](#)
- [Understanding Dynamic ARP Inspection, page 247](#)
- [Default Dynamic ARP Inspection Configuration, page 250](#)
- [Relative Priority of ARP ACLs and DHCP Snooping Entries, page 251](#)
- [Configuring ARP ACLs for Non-DHCP Environments , page 251](#)
- [Configuring Dynamic ARP Inspection in DHCP Environments, page 254](#)
- [Limiting the Rate of Incoming ARP Packets, page 257](#)
- [Performing Dynamic ARP Inspection Validation Checks, page 259](#)
- [Monitoring DAI, page 261](#)
- [Verifying the DAI Configuration, page 262](#)
- [Additional References, page 262](#)

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, private VLAN 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.

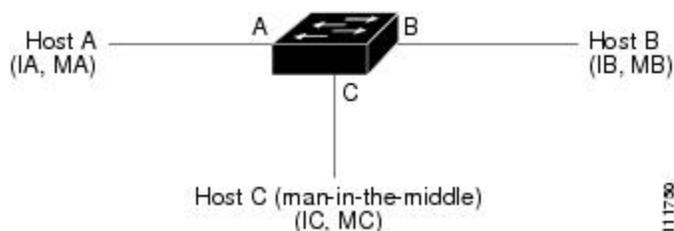
- When you enable dynamic ARP inspection on the switch, policers that were configured to police ARP traffic are no longer effective. The result is that all ARP traffic is sent to the CPU.
- When you configure dynamic ARP inspection smart logging, the contents of all packets in the log buffer (by default, all dropped packets) are sent to a NetFlow collector. If you configure this feature, make sure that smart logging is globally enabled.

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 15: 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.



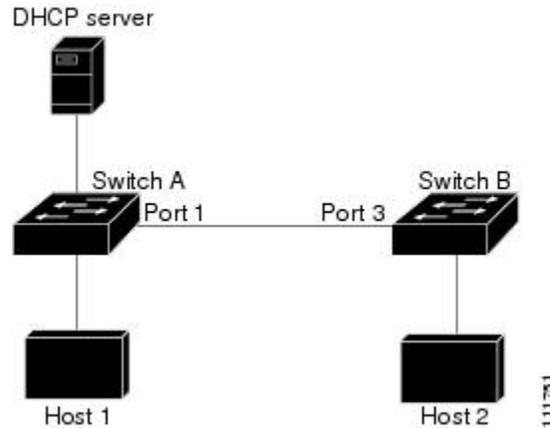
Caution

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.

Figure 16: ARP Packet Validation on a VLAN Enabled for Dynamic ARP Inspection



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.

**Note**

The rate limit for an EtherChannel is applied separately to each switch in a stack. For example, if a limit of 20 pps is configured on the EtherChannel, each switch with ports in the EtherChannel can carry up to 20 pps. If any switch exceeds the limit, the entire EtherChannel is placed into the error-disabled state.

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

Feature	Default Settings
Dynamic ARP inspection	Disabled on all VLANs.
Interface trust state	All interfaces are untrusted.
Rate limit of incoming ARP packets	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.
ARP ACLs for non-DHCP environments	No ARP ACLs are defined.
Validation checks	No checks are performed.

Feature	Default Settings
Log buffer	<p>When dynamic ARP inspection is enabled, all denied or dropped ARP packets are logged.</p> <p>The number of entries in the log is 32.</p> <p>The number of system messages is limited to 5 per second.</p> <p>The logging-rate interval is 1 second.</p>
Per-VLAN logging	All denied or dropped ARP packets are logged.

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **arp access-list *acl-name***
4. **permit ip host *sender-ip* mac host *sender-mac* [log]**
5. **exit**
6. **ip arp inspection filter *arp-acl-name* vlan *vlan-range* [static]**
7. **ip arp inspection smartlog**
8. **interface *interface-id***
9. **no ip arp inspection trust**
10. **end**
11. Use the following show commands:
 - **show arp access-list *acl-name***
 - **show ip arp inspection vlan *vlan-range***
 - **show ip arp inspection interfaces**
12. **show running-config**
13. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	arp access-list <i>acl-name</i>	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 <i>sender-ip</i> mac host <i>sender-mac</i> [log]	Permits ARP packets from the specified host (Host 2). <ul style="list-style-type: none"> • For <i>sender-ip</i>, enter the IP address of Host 2. • For <i>sender-mac</i>, enter the MAC address of Host 2.

	Command or Action	Purpose
		<ul style="list-style-type: none"> (Optional) Specifies the log to log a packet in the log buffer when it matches the access control entry (ACE). Matches are logged if you also configure the matchlog keyword in the ip arp inspection vlan logging global configuration command.
Step 5	exit	Returns to global configuration mode.
Step 6	ip arp inspection filter <i>arp-acl-name</i> vlan <i>vlan-range</i> [static]	<p>Applies ARP ACL to the VLAN. By default, no defined ARP ACLs are applied to any VLAN.</p> <ul style="list-style-type: none"> For <i>arp-acl-name</i>, specify the name of the ACL created in Step 2. For <i>vlan-range</i>, 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. <p>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.</p> <p>ARP packets containing only IP-to-MAC address bindings are compared against the ACL. Packets are permitted only if the access list permits them.</p>
Step 7	ip arp inspection smartlog	Specifies that whatever packets are currently being logged are also smart-logged. By default, all dropped packets are logged.
Step 8	interface <i>interface-id</i>	Specifies Switch A interface that is connected to Switch B, and enters the interface configuration mode.
Step 9	no ip arp inspection trust	<p>Configures Switch A interface that is connected to Switch B as untrusted.</p> <p>By default, all interfaces are untrusted.</p> <p>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 ip arp inspection vlan logging global configuration command.</p>
Step 10	end	Returns to privileged EXEC mode.
Step 11	<p>Use the following show commands:</p> <ul style="list-style-type: none"> show arp access-list <i>acl-name</i> show ip arp inspection vlan <i>vlan-range</i> 	Verifies your entries.

	Command or Action	Purpose
	<ul style="list-style-type: none"> • <code>show ip arp inspection interfaces</code> 	
Step 12	show running-config Example: <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 13	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

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.



Note

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.

SUMMARY STEPS

1. **enable**
2. **show cdp neighbors**
3. **configure terminal**
4. **ip arp inspection vlan *vlan-range***
5. **ip arp inspection smartlog**
6. **Interface *interface-id***
7. **ip arp inspection trust**
8. **end**
9. **show ip arp inspection interfaces**
10. **show ip arp inspection vlan *vlan-range***
11. **show ip dhcp snooping binding**
12. **show ip arp inspection statistics vlan *vlan-range***
13. **configure terminal**
14. **configure terminal**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	show cdp neighbors Example: SwitchController(config-if)# show cdp neighbors	Verify the connection between the switches.
Step 3	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 4	ip arp inspection vlan <i>vlan-range</i> Example: SwitchController(config)# ip arp inspection vlan 1	Enable dynamic ARP inspection on a per-VLAN basis. By default, dynamic ARP inspection is disabled on all VLANs. For <i>vlan-range</i> , 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.

	Command or Action	Purpose
Step 5	ip arp inspection smartlog Example:	(Optional). Specifies that whatever packets are currently being logged are also smart-logged. By default, all dropped packets are logged.
Step 6	Interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet1/0/1	Specifies the interface connected to the other switch, and enter interface configuration mode.
Step 7	ip arp inspection trust Example: SwitchController(config-if)# ip arp inspection trust	Configures the connection between the switches as trusted. By default, all interfaces are untrusted. 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 ip arp inspection vlan logging global configuration command.
Step 8	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.
Step 9	show ip arp inspection interfaces Example:	Verifies the dynamic ARP inspection configuration on interfaces.
Step 10	show ip arp inspection vlan <i>vlan-range</i> Example: SwitchController(config-if)# show ip arp inspection vlan 1	Verifies the dynamic ARP inspection configuration on VLAN.
Step 11	show ip dhcp snooping binding Example: SwitchController(config-if)# show ip dhcp snooping binding	Verifies the DHCP bindings.
Step 12	show ip arp inspection statistics vlan <i>vlan-range</i> Example: SwitchController(config-if)# show ip arp inspection statistics vlan 1	Checks the dynamic ARP inspection statistics on VLAN.

	Command or Action	Purpose
Step 13	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 14	configure terminal Example: SwitchController# configure terminal	Enters the 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **ip arp inspection limit {rate pps [burst interval seconds] | none}**
5. **exit**
6. Use the following commands:
 - **errdisable detect cause arp-inspection**
 - **errdisable recovery cause arp-inspection**
 - **errdisable recovery interval *interval***
7. **exit**
8. Use the following show commands:
 - **show ip arp inspection interfaces**
 - **show errdisable recovery**
9. **show running-config**
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	interface <i>interface-id</i>	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: <ul style="list-style-type: none"> • For ratepps, specify an upper limit for the number of incoming packets processed per second. The range is 0 to 2048 pps.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • (Optional) For burst interval <i>seconds</i>, specify the consecutive interval in seconds, over which the interface is monitored for a high rate of ARP packets. The range is 1 to 15. • For rate none, specify no upper limit for the rate of incoming ARP packets that can be processed.
Step 5	exit	Returns to global configuration mode.
Step 6	Use the following commands: <ul style="list-style-type: none"> • errdisable detect cause arp-inspection • errdisable recovery cause arp-inspection • errdisable recovery interval <i>interval</i> 	(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 <i>interval</i> , 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: <ul style="list-style-type: none"> • show ip arp inspection interfaces • show errdisable recovery 	Verifies your settings.
Step 9	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 10	copy running-config startup-config Example: SwitchController# 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip arp inspection validate** {[src-mac] [dst-mac] [ip]}
4. **exit**
5. **show ip arp inspection vlan** *vlan-range*
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	ip arp inspection validate {[src-mac] [dst-mac] [ip]}	<p>Performs a specific check on incoming ARP packets. By default, no checks are performed.</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>

	Command or Action	Purpose
Step 4	<code>exit</code>	Returns to privileged EXEC mode.
Step 5	<code>show ip arp inspection vlan</code> <i>vlan-range</i>	Verifies your settings.
Step 6	<code>show running-config</code> Example: SwitchController# <code>show</code> <code>running-config</code>	Verifies your entries.
Step 7	<code>copy running-config startup-config</code> Example: SwitchController# <code>copy</code> <code>running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Monitoring DAI

To monitor DAI, use the following commands:

Command	Description
<code>clear ip arp inspection statistics</code>	Clears dynamic ARP inspection statistics.
<code>show ip arp inspection statistics [vlan vlan-range]</code>	Displays statistics for forwarded, dropped, MAC validation failure, IP validation failure, ACL permitted and denied, and DHCP permitted and denied packets 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).
<code>clear ip arp inspection log</code>	Clears the dynamic ARP inspection log buffer.
<code>show ip arp inspection log</code>	Displays the configuration and contents of the dynamic ARP inspection log buffer.

For the `show ip arp inspection statistics` command, the switch increments the number of forwarded packets for each ARP request and response packet on a trusted dynamic ARP inspection port. The switch increments the number of ACL or DHCP permitted packets for each packet that is denied by source MAC, destination MAC, or IP validation checks, and the switch increments the appropriate.

Verifying the DAI Configuration

To display and verify the DAI configuration, use the following commands:

Command	Description
<code>show arp access-list [acl-name]</code>	Displays detailed information about ARP ACLs.
<code>show ip arp inspection interfaces [interface-id]</code>	Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.
<code>show ip arp inspection vlan vlan-range</code>	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).

Additional References

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

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/support</p>



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, page 265](#)
- [Information About 802.1x Port-Based Authentication, page 265](#)
- [How to Configure 802.1x Port-Based Authentication, page 299](#)
- [Monitoring 802.1x Statistics and Status, page 357](#)
- [Additional References, page 358](#)

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.

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.

**Note**

For complete syntax and usage information for the commands used in this chapter, see the “RADIUS Commands” section in the *Cisco IOS Security Command Reference, Release 12.4* and the command reference for this release.

Port-Based Authentication Process

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.

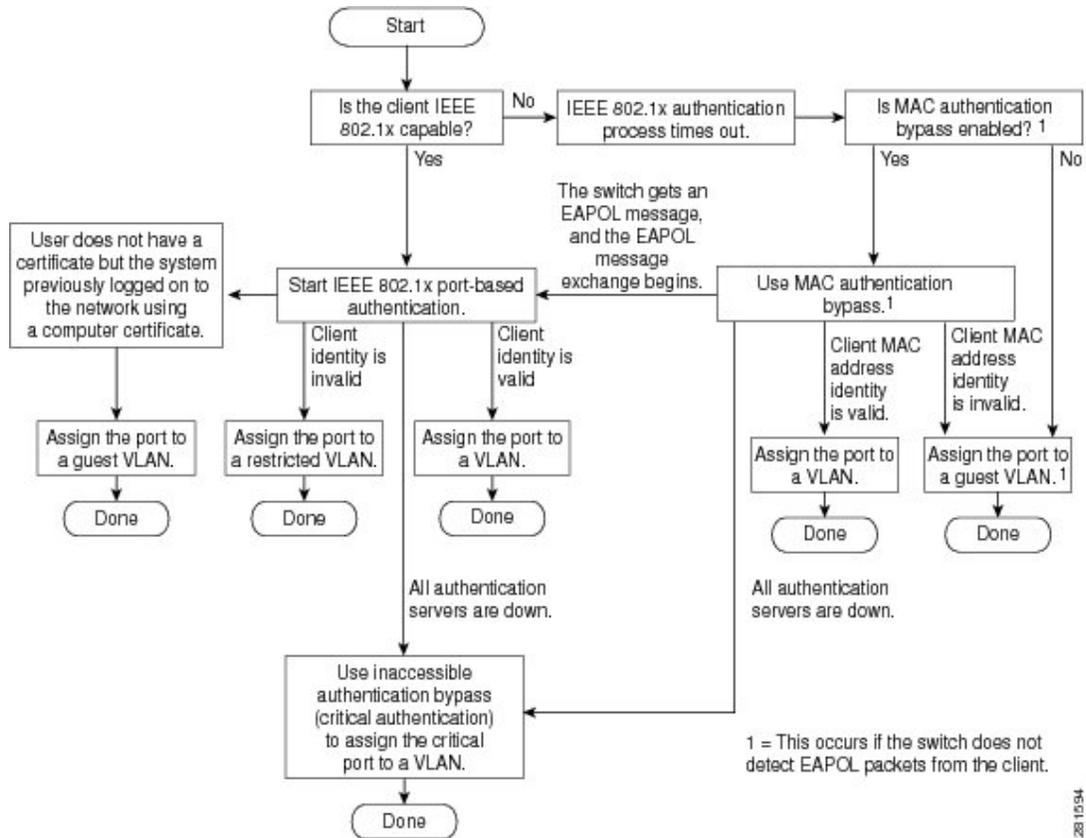
**Note**

Inaccessible authentication bypass is also referred to as critical authentication or the AAA fail 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.

Figure 17: Authentication Flowchart



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.



Note We recommend that you specify the attribute value as RADIUS-Request.

- 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

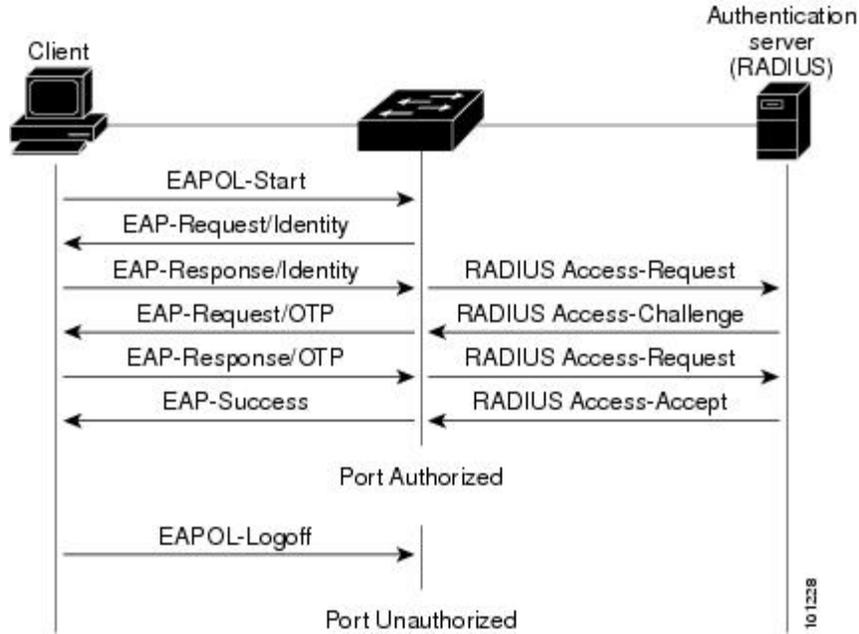
If 802.1x authentication is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client sends frames as if the port is in the authorized state. 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.

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.

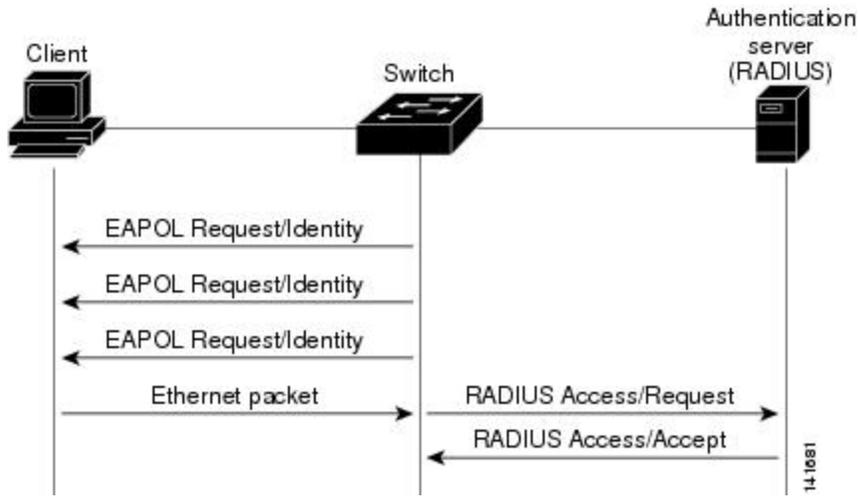
Figure 18: Message Exchange



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.

This figure shows the message exchange during MAC authentication bypass.

Figure 19: Message Exchange During MAC Authentication Bypass



Authentication Manager for Port-Based Authentication

Port-Based Authentication Methods

Table 25: 802.1x Features

Authentication method	Mode			
	Single host	Multiple host	MDA	Multiple Authentication
802.1x	VLAN assignment Per-user ACL Filter-ID attribute Downloadable ACL ⁹ Redirect URL	VLAN assignment	VLAN assignment Per-user ACL Filter-Id attribute Downloadable ACL Redirect URL	VLAN assignment Per-user ACL Filter-Id attribute Downloadable ACL Redirect URL

Authentication method	Mode			
	Single host	Multiple host	MDA	Multiple Authentication
MAC authentication bypass	VLAN assignment Per-user ACL Filter-ID attribute Downloadable ACL Redirect URL	VLAN assignment	VLAN assignment Per-user ACL Filter-Id attribute Downloadable ACL Redirect URL	VLAN assignment Per-user ACL Filter-Id attribute Downloadable ACL Redirect URL
Standalone web authentication	Proxy ACL, Filter-Id attribute, downloadable ACL			
NAC Layer 2 IP validation	Filter-Id attribute Downloadable ACL Redirect URL	Filter-Id attribute Downloadable ACL Redirect URL	Filter-Id attribute Downloadable ACL Redirect URL	Filter-Id attribute Downloadable ACL Redirect URL
Web authentication as fallback method ¹⁰	Proxy ACL Filter-Id attribute Downloadable ACL	Proxy ACL Filter-Id attribute Downloadable ACL	Proxy ACL Filter-Id attribute Downloadable ACL	Proxy ACL Filter-Id attribute Downloadable ACL

⁹ Supported in Cisco IOS Release 12.2(50)SE and later.

¹⁰ 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. However, the **dot1x system-authentication control** global configuration command only globally enables or disables 802.1x authentication.



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 26: Authentication Manager Commands and Earlier 802.1x Commands

The authentication manager commands in Cisco IOS Release 12.2(50)SE or later	The equivalent 802.1x commands in Cisco IOS Release 12.2(46)SE and earlier	Description
authentication control-direction {both in}	dot1x control-direction {both in}	Enable 802.1x authentication with the wake-on-LAN (WoL) feature, and configure the port control as unidirectional or bidirectional.
authentication event	dot1x auth-fail vlan dot1x critical (interface configuration) dot1x guest-vlan6	Enable the restricted VLAN on a port. Enable the inaccessible-authentication-bypass feature. Specify an active VLAN as an 802.1x guest VLAN.

The authentication manager commands in Cisco IOS Release 12.2(50)SE or later	The equivalent 802.1x commands in Cisco IOS Release 12.2(46)SE and earlier	Description
authentication fallback <i>fallback-profile</i>	dot1x fallback <i>fallback-profile</i>	Configure a port to use web authentication as a fallback method for clients that do not support 802.1x authentication.
authentication host-mode [multi-auth multi-domain multi-host single-host]	dot1x host-mode { single-host multi-host multi-domain }	Allow a single host (client) or multiple hosts on an 802.1x-authorized port.
authentication order	mab	Provides the flexibility to define the order of authentication methods to be used.
authentication periodic	dot1x reauthentication	Enable periodic re-authentication of the client.
authentication port-control { auto force-authorized force-un authorized }	dot1x port-control { auto force-authorized force-unauthorized }	Enable manual control of the authorization state of the port.
authentication timer	dot1x timeout	Set the 802.1x timers.
authentication violation { protect restrict shutdown }	dot1x violation-mode { shutdown restrict protect }	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.

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.

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.

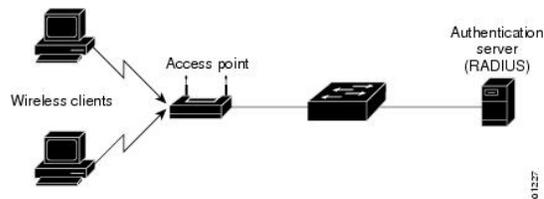
To avoid loss of connectivity to the RADIUS server, you should ensure that there is a redundant connection to it. For example, you can have a redundant connection to the stack master and another to a stack member, and if the stack master fails, the switch stack still has connectivity to the RADIUS server.

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 20: Multiple Host Mode Example



Note

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.



Note

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.



Note

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 mutli-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.



Note 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.



Note 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 27: Accounting AV Pairs

Attribute Number	AV Pair Name	START	INTERIM	STOP
Attribute[1]	User-Name	Always	Always	Always
Attribute[4]	NAS-IP-Address	Always	Always	Always
Attribute[5]	NAS-Port	Always	Always	Always
Attribute[8]	Framed-IP-Address	Never	Sometimes ¹¹	Sometimes
Attribute[25]	Class	Always	Always	Always
Attribute[30]	Called-Station-ID	Always	Always	Always
Attribute[31]	Calling-Station-ID	Always	Always	Always
Attribute[40]	Acct-Status-Type	Always	Always	Always
Attribute[41]	Acct-Delay-Time	Always	Always	Always
Attribute[42]	Acct-Input-Octets	Never	Always	Always
Attribute[43]	Acct-Output-Octets	Never	Always	Always

Attribute Number	AV Pair Name	START	INTERIM	STOP
Attribute[44]	Acct-Session-ID	Always	Always	Always
Attribute[45]	Acct-Authentic	Always	Always	Always
Attribute[46]	Acct-Session-Time	Never	Always	Always
Attribute[49]	Acct-Terminate-Cause	Never	Never	Always
Attribute[61]	NAS-Port-Type	Always	Always	Always

- ¹¹ The Framed-IP-Address AV pair is sent only if a valid Dynamic Host Control Protocol (DHCP) binding exists for the host in the DHCP snooping bindings table.

You can view the AV pairs that are being sent by the switch by entering the **debug radius accounting** privileged EXEC command.

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.

Related Topics

[Configuring 802.1x Readiness Check, on page 302](#)

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.

Related Topics

[Configuring the Switch-to-RADIUS-Server Communication, on page 311](#)

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

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

Attribute [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 `inacl#<n>` for the ingress direction and `outacl#<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. Because of limited support of Cisco IOS access lists on the switch, the Filter-Id attribute is supported only for IP ACLs numbered 1 to 199 and 1300 to 2699 (IP standard and 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.

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.

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.

**Note**

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.

**Note**

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.

**Note**

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.
- 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

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.

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 (multiauth) 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.

**Note**

Switch stacks are supported only on Catalyst 2960-S switches running the LAN base image.

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 is 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.

**Note**

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

**Note**

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.

**Note**

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
- VLAN Membership Policy Server (VMPS)—IEEE802.1x and VMPS are mutually exclusive.
- 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 cannot 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. 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.

Related Topics

[Configuring Flexible Authentication Ordering](#), on page 351

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.

**Note**

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.

Related Topics

[Configuring Open1x, on page 352](#)

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.

**Note**

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.

**Note**

You can assign a dynamic VLAN to a voice device on an MDA-enabled switch port, but the voice device fails authorization if a static voice VLAN configured on the switchport is the same as the dynamic VLAN assigned for the voice device in the RADIUS server.

- 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.
- You can use dynamic VLAN assignment from a RADIUS server only for data devices.
- 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.

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.
- 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 **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 **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 **dot1x supplicant controlled transient** command on a supplicant switch when BPDU guard is enabled on the authenticator switch port with the **spanning-tree bpduguard enable** interface configuration command.



Note

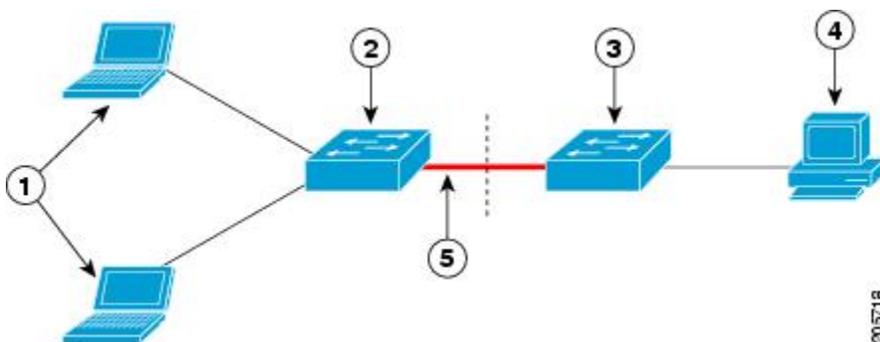
If you globally enable BPDU guard on the authenticator switch by using the **spanning-tree portfast bpduguard default** global configuration command, entering the **dot1x supplicant controlled transient** command does not prevent the BPDU violation.

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.

Use the **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 *device-traffic-class=switch* at the ACS. (You can configure this under the *group* or the *user* settings.)

Figure 21: Authenticator and Supplicant Switch using CISP



1	Workstations (clients)	2	Supplicant switch (outside wiring closet)
3	Authenticator switch	4	Access control server (ACS)
5	Trunk port		

**Note**

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

**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 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.

Related Topics

[Configuring Voice Aware 802.1x Security, on page 304](#)

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:

```
SwitchController# 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 1600000500000000B288508E5
```

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 28: Default 802.1x Authentication Configuration

Feature	Default Setting
Switch 802.1x enable state	Disabled.
Per-port 802.1x enable state	Disabled (force-authorized). The port sends and receives normal traffic without 802.1x-based authentication of the client.
AAA	Disabled.
RADIUS server <ul style="list-style-type: none"> • IP address • UDP authentication port • Key 	<ul style="list-style-type: none"> • None specified. • 1812. • None specified.
Host mode	Single-host mode.
Control direction	Bidirectional control.
Periodic re-authentication	Disabled.
Number of seconds between re-authentication attempts	3600 seconds.
Re-authentication number	2 times (number of times that the switch restarts the authentication process before the port changes to the unauthorized state).
Quiet period	60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client).
Retransmission time	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).

Feature	Default Setting
Maximum retransmission number	2 times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process).
Client timeout period	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.)
Authentication server timeout period	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.
Inactivity timeout	Disabled.
Guest VLAN	None specified.
Inaccessible authentication bypass	Disabled.
Restricted VLAN	None specified.
Authenticator (switch) mode	None specified.
MAC authentication bypass	Disabled.
Voice-aware security	Disabled.

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.
 - Dynamic-access ports—If you try to enable 802.1x authentication on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and 802.1x authentication is not enabled. If you try to change an 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration 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 multihosts 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.
- 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.

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 eapol-capable** privileged EXEC command without specifying an interface, all the ports on the switch stack are tested.
- When you configure the **dot1x test eapol-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 eapol-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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot1x test eapol-capable** [interface *interface-id*]
4. **dot1x test timeout** *timeout*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 3	dot1x test eapol-capable [interface <i>interface-id</i>] Example: <pre>SwitchController# 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</pre>	Enables the 802.1x readiness check on the switch. (Optional) For <i>interface-id</i> specify the port on which to check for IEEE 802.1x readiness. Note If you omit the optional interface keyword, all interfaces on the switch are tested.
Step 4	dot1x test timeout <i>timeout</i>	(Optional) Configures the timeout used to wait for EAPOL response. The range is from 1 to 65535 seconds. The default is 10 seconds.
Step 5	end Example: <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 6	show running-config Example: <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 7	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Related Topics

[802.1x Readiness Check, on page 280](#)

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:

SUMMARY STEPS

1. **configure terminal**
2. **errdisable detect cause security-violation shutdown vlan**
3. **errdisable recovery cause security-violation**
4. **clear errdisable interface interface-id vlan [vlan-list]**
5. Enter the following:
 - **shutdown**
 - **no shutdown**
6. **end**
7. **show errdisable detect**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
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.

	Command or Action	Purpose
Step 4	clear errdisable interface <i>interface-id</i> vlan [<i>vlan-list</i>]	(Optional) Reenable individual VLANs that have been error disabled. <ul style="list-style-type: none"> • For <i>interface-id</i> specify the port on which to reenable individual VLANs. • (Optional) For <i>vlan-list</i> specify a list of VLANs to be re-enabled. If <i>vlan-list</i> is not specified, all VLANs are re-enabled.
Step 5	Enter the following: <ul style="list-style-type: none"> • shutdown • no shutdown 	(Optional) Re-enable an error-disabled VLAN, and clear all error-disable indications.
Step 6	end	Return to privileged EXEC mode.
Step 7	show errdisable detect	Verify your entries.

This example shows how to configure the switch to shut down any VLAN on which a security violation error occurs:

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

This example shows how to re-enable all VLANs that were error disabled on port Gigabit Ethernet 40/2.

```
Switch# clear errdisable interface gigabitethernet4/0/2  
vlan
```

You can verify your settings by entering the **show errdisable detect** privileged EXEC command.

Related Topics

[Voice Aware 802.1x Security, on page 298](#)

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:

SUMMARY STEPS

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication dot1x {default} *method1***
4. **interface *interface-id***
5. **switchport mode access**
6. **authentication violation {shutdown | restrict | protect | replace}**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	aaa new-model Example: SwitchController(config)# aaa new-model	Enables AAA.
Step 3	aaa authentication dot1x {default} <i>method1</i> Example: SwitchController(config)# aaa authentication dot1x default group radius	<p>Creates an 802.1x authentication method list.</p> <p>To create a default list that is used when a named list is <i>not</i> specified in the authentication command, use the default keyword followed by the method that is to be used in default situations. The default method list is automatically applied to all ports.</p> <p>For <i>method1</i>, enter the group radius keywords to use the list of all RADIUS servers for authentication.</p> <p>Note Though other keywords are visible in the command-line help string, only the group radius keywords are supported.</p>
Step 4	interface <i>interface-id</i> Example: SwitchController(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: SwitchController(config-if)# switchport	Sets the port to access mode.

	Command or Action	Purpose
	<code>mode access</code>	
Step 6	<p>authentication violation {shutdown restrict protect replace}</p> <p>Example:</p> <pre>SwitchController(config-if) # authentication violation restrict</pre>	<p>Configures the violation mode. The keywords have these meanings:</p> <ul style="list-style-type: none"> • 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	<p>end</p> <p>Example:</p> <pre>SwitchController(config-if) # end</pre>	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.

SUMMARY STEPS

1. A user connects to a port on the switch.
2. Authentication is performed.
3. VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.
4. The switch sends a start message to an accounting server.
5. Re-authentication is performed, as necessary.
6. The switch sends an interim accounting update to the accounting server that is based on the result of re-authentication.
7. The user disconnects from the port.
8. The switch sends a stop message to the accounting server.

DETAILED STEPS

	Command or Action	Purpose
Step 1	A user connects to a port on the switch.	
Step 2	Authentication is performed.	
Step 3	VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.	
Step 4	The switch sends a start message to an accounting server.	
Step 5	Re-authentication is performed, as necessary.	
Step 6	The switch sends an interim accounting update to the accounting server that is based on the result of re-authentication.	
Step 7	The user disconnects from the port.	
Step 8	The switch sends a stop message to the accounting server.	

Configuring 802.1x Port-Based Authentication

Beginning in privileged EXEC mode, follow these steps to configure 802.1x port-based authentication:

SUMMARY STEPS

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication dot1x {default} *method1***
4. **dot1x system-auth-control**
5. **aaa authorization network {default} group radius**
6. **radius-server host *ip-address***
7. **radius-server key *string***
8. **interface *interface-id***
9. **switchport mode access**
10. **authentication port-control auto**
11. **dot1x pae authenticator**
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 2	<p>aaa new-model</p> <p>Example:</p> <pre>SwitchController(config)# aaa new-model</pre>	Enables AAA.
Step 3	<p>aaa authentication dot1x {default} method1</p> <p>Example:</p> <pre>SwitchController(config)# aaa authentication dot1x default group radius</pre>	<p>Creates an 802.1x authentication method list.</p> <p>To create a default list that is used when a named list is <i>not</i> specified in the authentication command, use the default keyword followed by the method that is to be used in default situations. The default method list is automatically applied to all ports.</p> <p>For <i>method1</i>, enter the group radius keywords to use the list of all RADIUS servers for authentication.</p> <p>Note Though other keywords are visible in the command-line help string, only the group radius keywords are supported.</p>
Step 4	<p>dot1x system-auth-control</p> <p>Example:</p> <pre>SwitchController(config)# dot1x system-auth-control</pre>	Enables 802.1x authentication globally on the switch.
Step 5	<p>aaa authorization network {default} group radius</p> <p>Example:</p> <pre>SwitchController(config)# aaa authorization network default group radius</pre>	<p>(Optional) Configures the switch to use user-RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.</p> <p>Note For per-user ACLs, single-host mode must be configured. This setting is the default.</p>
Step 6	<p>radius-server host ip-address</p> <p>Example:</p> <pre>SwitchController(config)# radius-server host 124.2.2.12</pre>	(Optional) Specifies the IP address of the RADIUS server.

	Command or Action	Purpose
Step 7	radius-server key <i>string</i> Example: SwitchController(config)# radius-server key abc1234	(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.
Step 8	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet1/0/2	Specifies the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.
Step 9	switchport mode access Example: SwitchController(config-if)# switchport mode access	(Optional) Sets the port to access mode only if you configured the RADIUS server in Step 6 and Step 7.
Step 10	authentication port-control auto Example: SwitchController(config-if)# authentication port-control auto	Enables 802.1x authentication on the port.
Step 11	dot1x pae authenticator Example: SwitchController(config-if)# dot1x pae authenticator	Sets the interface Port Access Entity to act only as an authenticator and ignore messages meant for a supplicant.
Step 12	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.

Configuring the Switch-to-RADIUS-Server Communication

You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using the **radius-server host** global configuration command. If you want to configure these options on a per-server basis, use the **radius-server timeout**, the **radius-server retransmit**, and the **radius-server key** global configuration commands.

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 the RADIUS server parameters on the switch. This procedure is required.

Before You Begin

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** *{hostname | ip-address}* **auth-port** *port-number* **key** *string*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	radius-server host <i>{hostname ip-address}</i> auth-port <i>port-number</i> key <i>string</i> Example: SwitchController (config) # radius-server host 125.5.5.43 auth-port 1812 key string	Configures the RADIUS server parameters. For <i>hostname ip-address</i> , specify the hostname or IP address of the remote RADIUS server. For auth-port <i>port-number</i> , specify the UDP destination port for authentication requests. The default is 1812. The range is 0 to 65536. For key <i>string</i> , 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. Note Always configure the key as the last item in the radius-server host command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. 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. If you want to use multiple RADIUS servers, re-enter this command.

	Command or Action	Purpose
Step 4	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.

Related Topics

[Switch-to-RADIUS-Server Communication, on page 280](#)

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet2/0/1	Specifies the port to which multiple hosts are indirectly attached, and enter interface configuration mode.
Step 3	authentication host-mode [multi-auth multi-domain multi-host single-host]	Allows multiple hosts (clients) on an 802.1x-authorized port. The keywords have these meanings:

	Command or Action	Purpose
	<p>Example:</p> <pre>SwitchController(config-if)# authentication host-mode multi-host</pre>	<ul style="list-style-type: none"> • multi-auth—Allow one client on the voice VLAN and multiple authenticated clients on the data VLAN. <p>Note The multi-auth keyword is only available with the authentication host-mode command.</p> <ul style="list-style-type: none"> • multi-host—Allow multiple hosts on an 802.1x-authorized port after a single host has been authenticated. • multi-domain—Allow both a host and a voice device, such as an IP phone (Cisco or non-Cisco), to be authenticated on an IEEE 802.1x-authorized port. <p>Note You must configure the voice VLAN for the IP phone when the host mode is set to multi-domain.</p> <p>Make sure that the authentication port-control interface configuration command is set to auto for the specified interface.</p>
Step 4	<p>end</p> <p>Example:</p> <pre>SwitchController(config-if)# end</pre>	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.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **authentication periodic**
4. **authentication timer** {{{inactivity | reauthenticate | restart}} {value}}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface interface-id Example: SwitchController(config)# interface gigabitethernet2/0/1	Specifies the port to be configured, and enter interface configuration mode.
Step 3	authentication periodic Example: SwitchController(config-if)# authentication periodic	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]} { <i>value</i> } Example: SwitchController(config-if)# authentication timer reauthenticate 180	Sets the number of seconds between re-authentication attempts. The authentication timer keywords have these meanings: <ul style="list-style-type: none"> • 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 This command affects the behavior of the switch only if periodic re-authentication is enabled.
Step 5	end Example: SwitchController(config-if)# end	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 inactivity** 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.

SUMMARY STEPS

1. **configure terminal**
2. **interface *interface-id***
3. **authentication timer inactivity *seconds***
4. **end**
5. **show authentication sessions interface *interface-id***
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet2/0/1	Specifies the port to be configured, and enter interface configuration mode.
Step 3	authentication timer inactivity <i>seconds</i> Example: SwitchController(config-if)# authentication timer inactivity 30	Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.
Step 4	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.
Step 5	show authentication sessions interface <i>interface-id</i> Example: SwitchController# show authentication sessions interface gigabitethernet2/0/1	Verifies your entries.

	Command or Action	Purpose
Step 6	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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.



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 change the amount of time that the switch waits for client notification. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **authentication timer reauthenticate** *seconds*
4. **end**
5. **show authentication sessions interface** *interface-id*
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController (config)# interface	Specifies the port to be configured, and enter interface configuration mode.

	Command or Action	Purpose
	<code>gigabitethernet2/0/1</code>	
Step 3	<p>authentication timer reauthenticate <i>seconds</i></p> <p>Example:</p> <pre>SwitchController(config-if)# authentication timer reauthenticate 60</pre>	<p>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.</p> <p>The range is 1 to 65535 seconds; the default is 5.</p>
Step 4	<p>end</p> <p>Example:</p> <pre>SwitchController(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 5	<p>show authentication sessions interface <i>interface-id</i></p> <p>Example:</p> <pre>SwitchController# show authentication sessions interface gigabitethernet2/0/1</pre>	Verifies your entries.
Step 6	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface *interface-id***
3. **dot1x max-reauth-req *count***
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet2/0/1	Specifies the port to be configured, and enter interface configuration mode.
Step 3	dot1x max-reauth-req <i>count</i> Example: SwitchController(config-if)# dot1x max-reauth-req 5	Sets the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. The range is 1 to 10; the default is 2.
Step 4	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.

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.


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 re-authentication number. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **dot1x max-req** *count*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController# interface gigabitethernet2/0/1	Specifies the port to be configured, and enter interface configuration mode.
Step 3	switchport mode access Example: SwitchController(config-if)# switchport mode access	Sets the port to access mode only if you previously configured the RADIUS server.
Step 4	dot1x max-req <i>count</i> Example: SwitchController(config-if)# dot1x max-req 4	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.
Step 5	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.

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.

SUMMARY STEPS

1. **configure terminal**
2. **authentication mac-move permit**
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 2	authentication mac-move permit Example: SwitchController(config)# authentication mac-move permit	Enables MAC move on the switch. Default is deny. In Session Aware Networking mode, the default CLI is access-session mac-move deny . To enable Mac Move in Session Aware Networking, use the no access-session mac-move global configuration command.
Step 3	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.
Step 4	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 5	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **authentication violation** {**protect** | **replace** | **restrict** | **shutdown**}
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet2/0/2	Specifies the port to be configured, and enter interface configuration mode.
Step 3	authentication violation { protect replace restrict shutdown } Example: SwitchController(config-if)# authentication violation replace	Use the replace keyword to enable MAC replace on the interface. The port removes the current session and initiates authentication with the new host. The other keywords have these effects: <ul style="list-style-type: none"> • 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.

	Command or Action	Purpose
Step 4	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.
Step 5	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 6	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface *interface-id***
3. **aaa accounting dot1x default start-stop group radius**
4. **aaa accounting system default start-stop group radius**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet1/0/3	Specifies the port to be configured, and enter interface configuration mode.
Step 3	aaa accounting dot1x default start-stop group radius Example: SwitchController(config-if)# aaa accounting dot1x default start-stop group radius	Enables 802.1x accounting using the list of all RADIUS servers.
Step 4	aaa accounting system default start-stop group radius Example: SwitchController(config-if)# aaa accounting system default start-stop group radius	(Optional) Enables system accounting (using the list of all RADIUS servers) and generates system accounting reload event messages when the switch reloads.
Step 5	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 7	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. Use one of the following:
 - **switchport mode access**
 - **switchport mode private-vlan host**
4. **authentication event no-response action authorize vlan** *vlan-id*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	<p><code>interface <i>interface-id</i></code></p> <p>Example:</p> <pre>SwitchController(config)# interface gigabitethernet2/0/2</pre>	Specifies the port to be configured, and enter interface configuration mode.
Step 3	<p>Use one of the following:</p> <ul style="list-style-type: none"> • <code>switchport mode access</code> • <code>switchport mode private-vlan host</code> <p>Example:</p> <pre>SwitchController(config-if)# switchport mode private-vlan host</pre>	<ul style="list-style-type: none"> • Sets the port to access mode. • Configures the Layer 2 port as a private-VLAN host port.
Step 4	<p><code>authentication event no-response action authorize vlan <i>vlan-id</i></code></p> <p>Example:</p> <pre>SwitchController(config-if)# authentication event no-response action authorize vlan 2</pre>	<p>Specifies an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094.</p> <p>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.</p>
Step 5	<p><code>end</code></p> <p>Example:</p> <pre>SwitchController(config-if)# end</pre>	Returns to privileged EXEC mode.

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface *interface-id***
3. Use one of the following:
 - **switchport mode access**
 - **switchport mode private-vlan host**
4. **authentication port-control auto**
5. **authentication event fail action authorize vlan *vlan-id***
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet2/0/2	Specifies the port to be configured, and enter interface configuration mode.
Step 3	Use one of the following: <ul style="list-style-type: none"> • switchport mode access • switchport mode private-vlan host Example: SwitchController(config-if)# switchport mode access	<ul style="list-style-type: none"> • Sets the port to access mode. • Configures the Layer 2 port as a private-VLAN host port.
Step 4	authentication port-control auto Example: SwitchController(config-if)# authentication port-control auto	Enables 802.1x authentication on the port.

	Command or Action	Purpose
Step 5	authentication event fail action authorize vlan <i>vlan-id</i> Example: <pre>SwitchController(config-if)# authentication event fail action authorize vlan 2</pre>	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: <pre>SwitchController(config-if)# end</pre>	Returns to privileged EXEC mode.

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface *interface-id***
3. Use one of the following:
 - **switchport mode access**
 - **switchport mode private-vlan host**
4. **authentication port-control auto**
5. **authentication event fail action authorize vlan *vlan-id***
6. **authentication event retry *retry count***
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet2/0/3	Specifies the port to be configured, and enter interface configuration mode.
Step 3	Use one of the following: <ul style="list-style-type: none"> • switchport mode access • switchport mode private-vlan host Example: or SwitchController(config-if)# switchport mode access	<ul style="list-style-type: none"> • Sets the port to access mode. • Configures the Layer 2 port as a private-VLAN host port.
Step 4	authentication port-control auto Example: SwitchController(config-if)# authentication port-control auto	Enables 802.1x authentication on the port.
Step 5	authentication event fail action authorize vlan <i>vlan-id</i> Example: SwitchController(config-if)# authentication event fail action authorize vlan 8	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	authentication event retry <i>retry count</i> Example: SwitchController(config-if)# authentication event retry 2	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.

	Command or Action	Purpose
Step 7	end Example: SwitchController(config-if) # end	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.

SUMMARY STEPS

1. **configure terminal**
2. **aaa new-model**
3. **radius-server dead-criteria** {time *seconds* } [*tries number*]
4. **radius-server deadtime** *minutes*
5. **radius-server host** *ip-address address* [*acct-port udp-port*] [*auth-port udp-port*] [*testusername name*] [*idle-time time*] [*ignore-acct-port*] [*ignore-auth-port*] [*key string*]
6. **dot1x critical** {*capol* | *recovery delay milliseconds*}
7. **interface** *interface-id*
8. **authentication event server dead action** {*authorize* | *reinitialize*} **vlan** *vlan-id*
9. **switchport voice vlan** *vlan-id*
10. **authentication event server dead action authorize voice**
11. **show authentication interface** *interface-id*
12. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	aaa new-model Example: <pre>SwitchController(config)# aaa new-model</pre>	Enables AAA.
Step 3	radius-server dead-criteria {time seconds } [tries number] Example: <pre>SwitchController(config)# radius-server dead-criteria time 20 tries 10</pre>	Sets the conditions that determine when a RADIUS server is considered un-available or down (dead). <ul style="list-style-type: none"> • time— 1 to 120 seconds. The switch dynamically determines a default <i>seconds</i> value between 10 and 60. • number—1 to 100 tries. The switch dynamically determines a default <i>triesnumber</i> between 10 and 100.
Step 4	radius-server deadtime minutes Example: <pre>SwitchController(config)# radius-server deadtime 60</pre>	(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.
Step 5	radius-server host ip-address address [acct-port udp-port] [auth-port udp-port] [testusername name [idle-time time] [ignore-acct-port] [ignore auth-port]] [key string] Example: <pre>SwitchController(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username user1 idle-time 30 key abc1234</pre>	(Optional) Configure the RADIUS server parameters by using these keywords: <ul style="list-style-type: none"> • acct-port udp-port—Specify the UDP port for the RADIUS accounting server. The range for the UDP port number is from 0 to 65536. The default is 1646. • auth-port udp-port—Specify the UDP port for the RADIUS authentication server. The range for the UDP port number is from 0 to 65536. The default is 1645. • Note You should configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to nondefault values. • test username name—Enable automated testing of the RADIUS server status, and specify the username to be used. • idle-time time—Set the interval of time in minutes after which the switch sends test packets to the server. The range is from 1 to 35791 minutes. The default is 60 minutes (1 hour). • ignore-acct-port—Disable testing on the RADIUS-server accounting port. • ignore-auth-port—Disable testing on the RADIUS-server authentication port. • For key string, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the

	Command or Action	Purpose
		<p>RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server.</p> <p>Note Always configure the key as the last item in the radius-server host command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. 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.</p> <p>You can also configure the authentication and encryption key by using theradius-server key {0string 7string string} global configuration command.</p>
Step 6	<p>dot1x critical {eapol recovery delay milliseconds}</p> <p>Example:</p> <pre>SwitchController(config)# dot1x critical eapol (config)# dot1x critical recovery delay 2000</pre>	<p>(Optional) Configure the parameters for inaccessible authentication bypass:</p> <ul style="list-style-type: none"> • eapol—Specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port. • 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).
Step 7	<p>interface interface-id</p> <p>Example:</p> <pre>SwitchController(config)# interface gigabitethernet 1/0/1</pre>	Specify the port to be configured, and enter interface configuration mode.
Step 8	<p>authentication event server dead action {authorize reinitialize} vlan vlan-id</p> <p>Example:</p> <pre>SwitchController(config-if)# authentication event server dead action reinitialicze vlan 20</pre>	<p>Use these keywords to move hosts on the port if the RADIUS server is unreachable:</p> <ul style="list-style-type: none"> • authorize—Move any new hosts trying to authenticate to the user-specified critical VLAN. • reinitialize—Move all authorized hosts on the port to the user-specified critical VLAN.
Step 9	<p>switchport voice vlan vlan-id</p> <p>Example:</p> <pre>SwitchController(config-if)# switchport voice vlan</pre>	Specifies the voice VLAN for the port. The voice VLAN cannot be the same as the critical data VLAN configured in Step 6.

	Command or Action	Purpose
Step 10	authentication event server dead action authorize voice Example: <pre>SwitchController(config-if)# authentication event server dead action authorize voice</pre>	Configures critical voice VLAN to move data traffic on the port to the voice VLAN if the RADIUS server is unreachable.
Step 11	show authentication interface <i>interface-id</i> Example: <pre>SwitchController(config-if)# do show authentication interface gigabit 1/0/1</pre>	(Optional) Verify your entries.
Step 12	copy running-config startup-config Example: <pre>SwitchController(config-if)# do copy running-config startup-config</pre>	(Optional) Verify your entries.

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 host** 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:

```
SwitchController(config)# radius-server dead-criteria time 30 tries 20
SwitchController(config)# radius-server deadtime 60
SwitchController(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test
username user1 idle-time 30 key abc1234
SwitchController(config)# dot1x critical eapol
SwitchController(config)# dot1x critical recovery delay 2000
SwitchController(config)# interface gigabitethernet 1/0/1
SwitchController(config-if)# dot1x critical
SwitchController(config-if)# dot1x critical recovery action reinitialize
SwitchController(config-if)# dot1x critical vlan 20
SwitchController(config-if)# end
```

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **authentication control-direction** {**both** | **in**}
4. **end**
5. **show authentication sessions interface** *interface-id*
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet2/0/3	Specifies the port to be configured, and enter interface configuration mode.
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. <ul style="list-style-type: none"> • 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.
Step 4	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	show authentication sessions interface <i>interface-id</i> Example: <pre>SwitchController# show authentication sessions interface gigabitethernet2/0/3</pre>	Verifies your entries.
Step 6	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring MAC Authentication Bypass

Beginning in privileged EXEC mode, follow these steps to enable MAC authentication bypass. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **interface *interface-id***
3. **authentication port-control auto**
4. **mab [eap]**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 2	interface <i>interface-id</i> Example: <pre>SwitchController(config)# interface gigabitethernet2/0/1</pre>	Specifies the port to be configured, and enter interface configuration mode.

	Command or Action	Purpose
Step 3	authentication port-control auto Example: <pre>SwitchController(config-if)# authentication port-control auto</pre>	Enables 802.1x authentication on the port.
Step 4	mab [eap] Example: <pre>SwitchController(config-if)# mab</pre>	Enables MAC authentication bypass. (Optional) Use the eap keyword to configure the switch to use EAP for authorization.
Step 5	end Example: <pre>SwitchController(config-if)# end</pre>	Returns to privileged EXEC mode.

Formatting a MAC Authentication Bypass Username and Password

Use the optional **mab request format** command to format the MAB username and password in a style accepted by the authentication server. The username and password are usually the MAC address of the client. Some authentication server configurations require the password to be different from the username.

Beginning in privileged EXEC mode, follow these steps to format MAC authentication bypass username and passwords.

SUMMARY STEPS

1. **configure terminal**
2. **mab request format attribute 1 groupsize {1 | 2 | 4 | 12} [separator {- | : | .} {lowercase | uppercase}]**
3. **mab request format attribute2 {0 | 7} text**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	<p>mab request format attribute 1 groupsize {1 2 4 12} [separator {- : .}] {lowercase uppercase}]</p> <p>Example:</p> <pre>SwitchController(config)# mab request format attribute 1 groupsize 12</pre>	<p>Specifies the format of the MAC address in the User-Name attribute of MAB-generated Access-Request packets.</p> <p>1—Sets the username format of the 12 hex digits of the MAC address.</p> <p>group size—The number of hex nibbles to concatenate before insertion of a separator. A valid groupsize must be either 1, 2, 4, or 12.</p> <p>separator—The character that separates the hex nibbles according to group size. A valid separator must be either a hyphen, colon, or period. No separator is used for a group size of 12.</p> <p>{lowercase uppercase}—Specifies if nonnumeric hex nibbles should be in lowercase or uppercase.</p>
Step 3	<p>mab request format attribute2 {0 7} <i>text</i></p> <p>Example:</p> <pre>SwitchController(config)# mab request format attribute 2 7 A02f44E18B12</pre>	<p>2—Specifies a custom (nondefault) value for the User-Password attribute in MAB-generated Access-Request packets.</p> <p>0—Specifies a cleartext password to follow.</p> <p>7—Specifies an encrypted password to follow.</p> <p><i>text</i>—Specifies the password to be used in the User-Password attribute.</p> <p>Note When you send configuration information in e-mail, remove type 7 password information. The show tech-support command removes this information from its output by default.</p>
Step 4	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	<p>Returns to privileged EXEC mode.</p>

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:

SUMMARY STEPS

1. **configure terminal**
2. **vlan group** *vlan-group-name* **vlan-list** *vlan-list*
3. **end**
4. **no vlan group** *vlan-group-name* **vlan-list** *vlan-list*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	vlan group <i>vlan-group-name</i> vlan-list <i>vlan-list</i> Example: SwitchController(config)# vlan group eng-dept vlan-list 10	Configures a VLAN group, and maps a single VLAN or a range of VLANs to it.
Step 3	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.
Step 4	no vlan group <i>vlan-group-name</i> vlan-list <i>vlan-list</i> Example: SwitchController(config)# no vlan group eng-dept vlan-list 10	Clears the VLAN group configuration or elements of the VLAN group configuration.

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:

```
SwitchController(config)# vlan group eng-dept vlan-list 10

SwitchController(config)# show vlan group group-name eng-dept
Group Name                Vlans Mapped
-----
eng-dept                   10

SwitchController(config)# show dot1x vlan-group all
Group Name                Vlans Mapped
-----
eng-dept                   10
hr-dept                    20
```

This example shows how to add a VLAN to an existing VLAN group and to verify that the VLAN was added:

```
SwitchController(config)# vlan group eng-dept vlan-list 30
SwitchController(config)# show vlan group eng-dept
Group Name                Vlans Mapped
```

```
-----
eng-dept                               10,30
-----
```

This example shows how to remove a VLAN from a VLAN group:

```
SwitchController# 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:

```
SwitchController(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.
```

```
SwitchController(config)# show vlan group group-name eng-dept
```

This example shows how to clear all the VLAN groups:

```
SwitchController(config)# no vlan group eng-dept vlan-list all
SwitchController(config)# show vlan-group all
```

For more information about these commands, see the *Cisco IOS Security Command Reference*.

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface *interface-id***
3. **switchport mode access**
4. **authentication event no-response action authorize vlan *vlan-id***
5. **authentication periodic**
6. **authentication timer reauthenticate**
7. **end**
8. **show authentication sessions interface *interface-id***
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 2	interface <i>interface-id</i> Example: <pre>SwitchController(config)# interface gigabitethernet2/0/3</pre>	Specifies the port to be configured, and enter interface configuration mode.
Step 3	switchport mode access Example: <pre>SwitchController(config-if)# switchport mode access</pre>	Sets the port to access mode only if you configured the RADIUS server.
Step 4	authentication event no-response action authorize vlan <i>vlan-id</i> Example: <pre>SwitchController(config-if)# authentication event no-response action authorize vlan 8</pre>	<p>Specifies an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094.</p> <p>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.</p>
Step 5	authentication periodic Example: <pre>SwitchController(config-if)# authentication periodic</pre>	Enables periodic re-authentication of the client, which is disabled by default.
Step 6	authentication timer reauthenticate Example: <pre>SwitchController(config-if)# authentication timer reauthenticate</pre>	<p>Sets re-authentication attempt for the client (set to one hour).</p> <p>This command affects the behavior of the switch only if periodic re-authentication is enabled.</p>
Step 7	end Example: <pre>SwitchController(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 8	show authentication sessions interface <i>interface-id</i> Example: <pre>SwitchController# show authentication sessions interface gigabitethernet2/0/3</pre>	Verifies your entries.

	Command or Action	Purpose
Step 9	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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:

SUMMARY STEPS

1. **configure terminal**
2. **cisp enable**
3. **interface *interface-id***
4. **switchport mode access**
5. **authentication port-control auto**
6. **dot1x pae authenticator**
7. **spanning-tree portfast**
8. **end**
9. **show running-config interface *interface-id***
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 2	cisp enable Example: SwitchController(config)# cisp enable	Enables CISP.
Step 3	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet2/0/1	Specifies the port to be configured, and enter interface configuration mode.
Step 4	switchport mode access Example: SwitchController(config-if)# switchport mode access	Sets the port mode to access .
Step 5	authentication port-control auto Example: SwitchController(config-if)# authentication port-control auto	Sets the port-authentication mode to auto.
Step 6	dot1x pae authenticator Example: SwitchController(config-if)# dot1x pae authenticator	Configures the interface as a port access entity (PAE) authenticator.
Step 7	spanning-tree portfast Example: SwitchController(config-if)# spanning-tree portfast trunk	Enables Port Fast on an access port connected to a single workstation or server..
Step 8	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.
Step 9	show running-config interface <i>interface-id</i> Example: SwitchController# show running-config interface	Verifies your configuration.

	Command or Action	Purpose
	<code>gigabitethernet2/0/1</code>	
Step 10	copy running-config startup-config Example: SwitchController# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Configuring a Supplicant Switch with NEAT

Beginning in privileged EXEC mode, follow these steps to configure a switch as a supplicant:

SUMMARY STEPS

1. `configure terminal`
2. `cisp enable`
3. `dot1x credentials profile`
4. `username suppswitch`
5. `password password`
6. `dot1x supplicant force-multicast`
7. `interface interface-id`
8. `switchport trunk encapsulation dot1q`
9. `switchport mode trunk`
10. `dot1x pae supplicant`
11. `dot1x credentials profile-name`
12. `end`
13. `show running-config interface interface-id`
14. `copy running-config startup-config`
15. Configuring NEAT with Auto Smartports Macros

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# <code>configure terminal</code>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	cisp enable Example: SwitchController(config)# cisp enable	Enables CISP.
Step 3	dot1x credentials <i>profile</i> Example: SwitchController(config)# dot1x credentials test	Creates 802.1x credentials profile. This must be attached to the port that is configured as supplicant.
Step 4	username <i>suppswitch</i> Example: SwitchController(config)# username suppswitch	Creates a username.
Step 5	password <i>password</i> Example: SwitchController(config)# password myswitch	Creates a password for the new username.
Step 6	dot1x supplicant force-multicast Example: SwitchController(config)# dot1x supplicant force-multicast	<p>Forces the switch to send only multicast EAPOL packets when it receives either unicast or multicast packets.</p> <p>This also allows NEAT to work on the supplicant switch in all host modes.</p>
Step 7	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet1/0/1	Specifies the port to be configured, and enter interface configuration mode.
Step 8	switchport trunk encapsulation dot1q Example: SwitchController(config-if)# switchport trunk encapsulation dot1q	Sets the port to trunk mode.
Step 9	switchport mode trunk Example: SwitchController(config-if)# switchport mode trunk	Configures the interface as a VLAN trunk port.

	Command or Action	Purpose
Step 10	dot1x pae supplicant Example: SwitchController(config-if)# dot1x pae supplicant	Configures the interface as a port access entity (PAE) supplicant.
Step 11	dot1x credentials profile-name Example: SwitchController(config-if)# dot1x credentials test	Attaches the 802.1x credentials profile to the interface.
Step 12	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.
Step 13	show running-config interface interface-id Example: SwitchController# show running-config interface gigabitethernet1/0/1	Verifies your configuration.
Step 14	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.
Step 15	Configuring NEAT with Auto Smartports Macros	You can also use an Auto Smartports user-defined macro instead of the switch VSA to configure the authenticator switch. For more information, see the <i>Auto Smartports Configuration Guide</i> for this release.

Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs

In addition to configuring 802.1x authentication on the switch, you need to configure the ACS. For more information, see the *Configuration Guide for Cisco Secure ACS 4.2*:
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs_config.pdf

**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:

SUMMARY STEPS

1. **configure terminal**
2. **ip device tracking**
3. **aaa new-model**
4. **aaa authorization network default local group radius**
5. **radius-server vsa send authentication**
6. **interface *interface-id***
7. **ip access-group *acl-id* in**
8. **show running-config interface *interface-id***
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 2	ip device tracking Example: SwitchController(config)# ip device tracking	Sets the ip device tracking table.
Step 3	aaa new-model Example: SwitchController(config)# aaa new-model	Enables AAA.

	Command or Action	Purpose
Step 4	aaa authorization network default local group radius Example: <pre>SwitchController(config)# aaa authorization network default local group radius</pre>	Sets the authorization method to local. To remove the authorization method, use the no aaa authorization network default local group radius command.
Step 5	radius-server vsa send authentication Example: <pre>SwitchController(config)# radius-server vsa send authentication</pre>	Configures the radius vsa send authentication.
Step 6	interface interface-id Example: <pre>SwitchController(config)# interface gigabitethernet2/0/4</pre>	Specifies the port to be configured, and enter interface configuration mode.
Step 7	ip access-group acl-id in Example: <pre>SwitchController(config-if)# ip access-group default_acl in</pre>	Configures the default ACL on the port in the input direction. Note The <i>acl-id</i> is an access list name or number.
Step 8	show running-config interface interface-id Example: <pre>SwitchController(config-if)# show running-config interface gigabitethernet2/0/4</pre>	Verifies your configuration.
Step 9	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring a Downloadable Policy

Beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **access-list *access-list-number* { deny | permit } { hostname | any | host } log**
3. **interface *interface-id***
4. **ip access-group *acl-id* in**
5. **exit**
6. **aaa new-model**
7. **aaa authorization network default group radius**
8. **ip device tracking**
9. **ip device tracking probe [count | interval | use-svi]**
10. **radius-server vsa send authentication**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 2	<p>access-list <i>access-list-number</i> { deny permit } { hostname any host } log</p> <p>Example:</p> <pre>SwitchController(config)# access-list 1 deny any log</pre>	<p>Defines the default port ACL.</p> <p>The access-list-number is a decimal number from 1 to 99 or 1300 to 1999.</p> <p>Enter deny or permit to specify whether to deny or permit access if conditions are matched.</p> <p>The source is the source address of the network or host that sends a packet, such as this:</p> <ul style="list-style-type: none"> • hostname: The 32-bit quantity in dotted-decimal format. • any: The keyword any as an abbreviation for source and source-wildcard value of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard value. • host: The keyword host as an abbreviation for source and source-wildcard of source 0.0.0.0. <p>(Optional) Applies the source-wildcard wildcard bits to the source.</p> <p>(Optional) Enters log to cause an informational logging message about the packet that matches the entry to be sent to the console.</p>

	Command or Action	Purpose
Step 3	interface <i>interface-id</i> Example: <pre>SwitchController(config)# interface gigabitethernet2/0/2</pre>	Enters interface configuration mode.
Step 4	ip access-group <i>acl-id</i> in Example: <pre>SwitchController(config-if)# ip access-group default_acl in</pre>	Configures the default ACL on the port in the input direction. Note The <i>acl-id</i> is an access list name or number.
Step 5	exit Example: <pre>SwitchController(config-if)# exit</pre>	Returns to global configuration mode.
Step 6	aaa new-model Example: <pre>SwitchController(config)# aaa new-model</pre>	Enables AAA.
Step 7	aaa authorization network default group radius Example: <pre>SwitchController(config)# aaa authorization network default group radius</pre>	Sets the authorization method to local. To remove the authorization method, use the no aaa authorization network default group radius command.
Step 8	ip device tracking Example: <pre>SwitchController(config)# ip device tracking</pre>	Enables the IP device tracking table. To disable the IP device tracking table, use the no ip device tracking global configuration commands.
Step 9	ip device tracking probe [count interval use-svi] Example: <pre>SwitchController(config)# ip device tracking probe count</pre>	(Optional) Configures the IP device tracking table: <ul style="list-style-type: none"> • count <i>count</i>—Sets the number of times that the switch sends the ARP probe. The range is from 1 to 5. The default is 3. • interval <i>interval</i>—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.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • use-svi—Uses the switch virtual interface (SVI) IP address as source of ARP probes.
Step 10	radius-server vsa send authentication Example: <pre>SwitchController(config)# radius-server vsa send authentication</pre>	Configures the network access server to recognize and use vendor-specific attributes. Note The downloadable ACL must be operational.
Step 11	end Example: <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.

Configuring VLAN ID-based MAC Authentication

Beginning in privileged EXEC mode, follow these steps:

SUMMARY STEPS

1. **configure terminal**
2. **mab request format attribute 32 vlan access-vlan**
3. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>SwitchController# configure terminal</pre>	Enters global configuration mode.
Step 2	mab request format attribute 32 vlan access-vlan Example: <pre>SwitchController(config)# mab request format attribute 32 vlan access-vlan</pre>	Enables VLAN ID-based MAC authentication.

	Command or Action	Purpose
Step 3	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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.



Note

Before changing the default order and priority of these authentication methods, however, you should understand the potential consequences of those changes. See http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/application_note_c27-573287_ps6638_Products_White_Paper.html for details.

Beginning in privileged EXEC mode, follow these steps:

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **authentication order** [**dot1x** | **mab**] | {webauth}
5. **authentication priority** [**dot1x** | **mab**] | {webauth}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet 1/0/1	Specifies the port to be configured, and enter interface configuration mode.
Step 3	switchport mode access Example: SwitchController(config-if)# switchport mode access	Sets the port to access mode only if you previously configured the RADIUS server.
Step 4	authentication order [dot1x mab] { webauth } Example: SwitchController(config-if)# authentication order mab dot1x	(Optional) Sets the order of authentication methods used on a port.
Step 5	authentication priority [dot1x mab] { webauth } Example: SwitchController(config-if)# authentication priority mab dot1x	(Optional) Adds an authentication method to the port-priority list.
Step 6	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.

Related Topics

[Flexible Authentication Ordering](#), on page 294

Configuring Open1x

Beginning in privileged EXEC mode, follow these steps to enable manual control of the port authorization state:

SUMMARY STEPS

1. **configure terminal**
2. **interface *interface-id***
3. **switchport mode access**
4. **authentication control-direction {both | in}**
5. **authentication fallback *name***
6. **authentication host-mode [multi-auth | multi-domain | multi-host | single-host]**
7. **authentication open**
8. **authentication order [dot1x | mab] | {webauth}**
9. **authentication periodic**
10. **authentication port-control {auto | force-authorized | force-un authorized}**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet 1/0/1	Specifies the port to be configured, and enter interface configuration mode.
Step 3	switchport mode access Example: SwitchController(config-if)# switchport mode access	Sets the port to access mode only if you configured the RADIUS server.
Step 4	authentication control-direction {both in} Example: SwitchController(config-if)# authentication control-direction both	(Optional) Configures the port control as unidirectional or bidirectional.

	Command or Action	Purpose
Step 5	authentication fallback <i>name</i> Example: <pre>SwitchController(config-if)# authentication fallback profile1</pre>	(Optional) Configures a port to use web authentication as a fallback method for clients that do not support 802.1x authentication.
Step 6	authentication host-mode [multi-auth multi-domain multi-host single-host] Example: <pre>SwitchController(config-if)# authentication host-mode multi-auth</pre>	(Optional) Sets the authorization manager mode on a port.
Step 7	authentication open Example: <pre>SwitchController(config-if)# authentication open</pre>	(Optional) Enables or disable open access on a port.
Step 8	authentication order [dot1x mab] {webauth} Example: <pre>SwitchController(config-if)# authentication order dot1x webauth</pre>	(Optional) Sets the order of authentication methods used on a port.
Step 9	authentication periodic Example: <pre>SwitchController(config-if)# authentication periodic</pre>	(Optional) Enables or disable reauthentication on a port.
Step 10	authentication port-control {auto force-authorized force-un authorized} Example: <pre>SwitchController(config-if)# authentication port-control auto</pre>	(Optional) Enables manual control of the port authorization state.
Step 11	end Example: <pre>SwitchController(config-if)# end</pre>	Returns to privileged EXEC mode.

Related Topics

[Open1x Authentication](#), on page 294

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **no dot1x pae authenticator**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet2/0/1	Specifies the port to be configured, and enter interface configuration mode.
Step 3	switchport mode access Example: SwitchController(config-if)# switchport mode access	(Optional) Sets the port to access mode only if you configured the RADIUS server.
Step 4	no dot1x pae authenticator Example: SwitchController(config-if)# no dot1x pae authenticator	Disables 802.1x authentication on the port.

	Command or Action	Purpose
Step 5	end Example: SwitchController(config-if)# end	Returns to privileged EXEC mode.

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface *interface-id***
3. **dot1x default**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet1/0/2	Enters interface configuration mode, and specify the port to be configured.
Step 3	dot1x default Example: SwitchController(config-if)# dot1x default	Resets the 802.1x parameters to the default values.

	Command or Action	Purpose
Step 4	end Example: SwitchController(config-if) # end	Returns to privileged EXEC mode.

Monitoring 802.1x Statistics and Status

Table 29: Privileged EXEC show Commands

Command	Purpose
show dot1x all statistics	Displays 802.1x statistics for all ports
show dot1x interface <i>interface-id</i> statistics	Displays 802.1x statistics for a specific port
show dot1x all [count details statistics summary]	Displays the 802.1x administrative and operational status for a switch
show dot1x interface <i>interface-id</i>	Displays the 802.1x administrative and operational status for a specific port

Table 30: Global Configuration Commands

Command	Purpose
no dot1x logging verbose	Filters verbose 802.1x authentication messages (beginning with Cisco IOS Release 12.2(55)SE)

For detailed information about the fields in these displays, see the command reference for this release.

Additional References

Related Documents

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.html
Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850-library.html

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

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/support</p>



CHAPTER 17

Configuring Web-Based Authentication

This chapter describes how to configure web-based authentication on the switch. It contains these sections:

- [Finding Feature Information, page 361](#)
- [Information About Web-Based Authentication, page 361](#)
- [How to Configure Web-Based Authentication, page 370](#)
- [Monitoring Web-Based Authentication Status, page 387](#)

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 Web-Based Authentication

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. Layer 3 interfaces are not supported on switches running the LAN base feature set.

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.

These sections describe the role of web-based authentication as part of AAA:

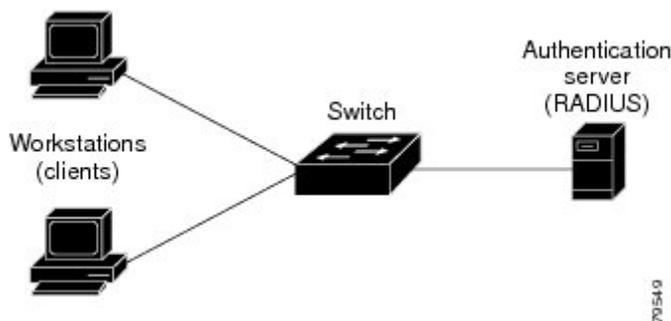
Device Roles

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 Java Script 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.

This figure shows the roles of these devices in a network.

Figure 22: Web-Based Authentication Device Roles



Host Detection

The switch maintains an IP device tracking table to store information about detected hosts.



Note

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.

By default, the IP device tracking feature is enabled on a switch.

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.
- 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:

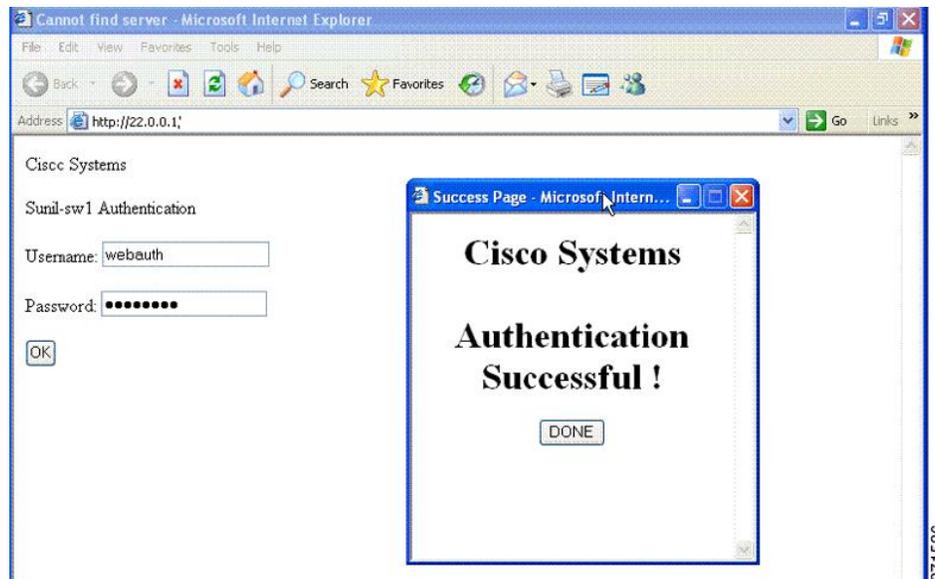
- *Authentication Successful*
- *Authentication Failed*
- *Authentication Expired*

The Local Web Authentication Banner can be configured in legacy and new-style (Session-aware) 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 23: Authentication Successful Banner

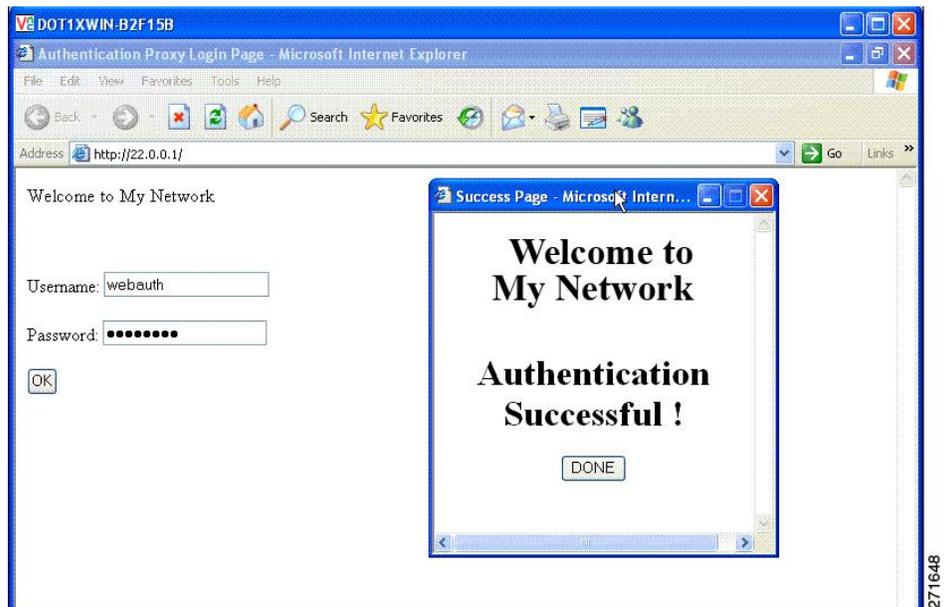


The banner can be customized as follows:

- 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.

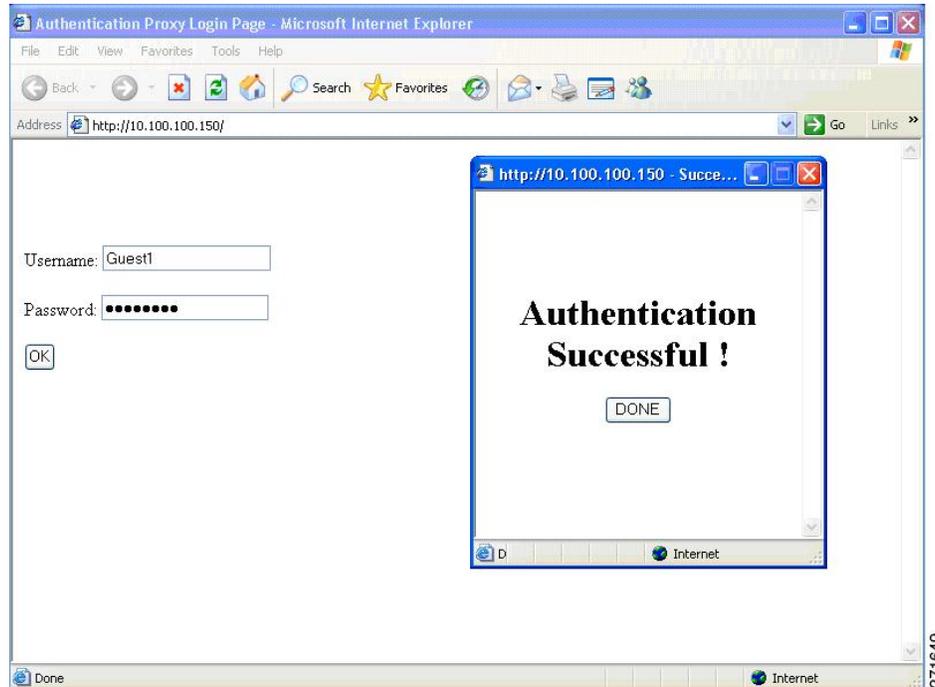
- New-style mode—Use the **parameter-map type webauth global banner** global configuration command
- Add a logo or text file to the banner :
 - Legacy mode—Use the **ip admission auth-proxy-banner http file-path** global configuration command.
 - New-style mode—Use the **parameter-map type webauth global banner** global configuration command

Figure 24: 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.

Figure 25: Login Screen With No Banner



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.

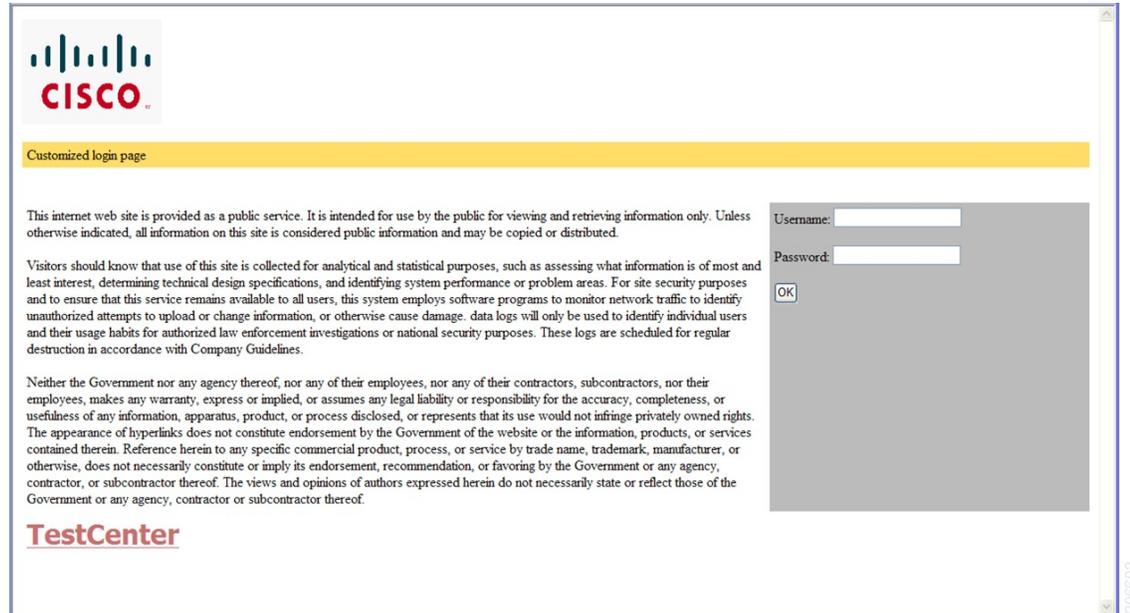
Guidelines

- 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 26: 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 379

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 381

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](#), on page 408

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.

EtherChannel

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 31: Default Web-based Authentication Configuration

Feature	Default Setting
AAA	Disabled

Feature	Default Setting
RADIUS server <ul style="list-style-type: none"> • IP address • UDP authentication port • Key 	<ul style="list-style-type: none"> • None specified • 1812 • None specified
Default value of inactivity timeout	3600 seconds
Inactivity timeout	Enabled

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.
- You must configure the default ACL on the interface before configuring web-based authentication. Configure a port ACL for a Layer 2 interface or a Cisco IOS ACL for a Layer 3 interface.
- 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 is not supported for IPv6 traffic.
- 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.
- 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 (DAACL). For more information, see the RADIUS server documentation.

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name *name* proxy http**
4. **interface *type slot/port***
5. **ip access-group *name***
6. **ip admission *name***
7. **exit**
8. **ip device tracking**
9. **end**
10. **show ip admission statusconfiguration**
11. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	ip admission name <i>name</i> proxy http Example: SwitchController(config)# ip admission name webauth1 proxy http	Configures an authentication rule for web-based authorization.
Step 4	interface <i>type slot/port</i> Example: SwitchController(config)# interface gigabitEthernet1/0/1	Enters interface configuration mode and specifies the ingress Layer 2 or Layer 3 interface to be enabled for web-based authentication. <i>type</i> can be fastethernet, gigabit ethernet, or tengigabitethernet.
Step 5	ip access-group <i>name</i> Example: SwitchController(config-if)# ip access-group	Applies the default ACL.

	Command or Action	Purpose
	<code>webauthag</code>	
Step 6	<p>ip admission <i>name</i></p> <p>Example:</p> <pre>SwitchController(config-if)# ip admission webauth1</pre>	Configures web-based authentication on the specified interface.
Step 7	<p>exit</p> <p>Example:</p> <pre>SwitchController(config-if)# exit</pre>	Returns to configuration mode.
Step 8	<p>ip device tracking</p> <p>Example:</p> <pre>SwitchController(config)# ip device tracking</pre>	Enables the IP device tracking table.
Step 9	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 10	<p>show ip admission statusconfiguration</p> <p>Example:</p> <pre>SwitchController# show ip admission statusconfiguration</pre>	Displays the configuration.
Step 11	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring AAA Authentication

Follow these steps to configure AAA authentication:

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa authentication login default group {tacacs+ | radius}
5. aaa authorization auth-proxy default group {tacacs+ | radius}
6. tacacs-server host {hostname | ip_address}
7. tacacs-server key {key-data}
8. end
9. show running-config
10. copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>SwitchController> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p>aaa new-model</p> <p>Example:</p> <pre>SwitchController(config)# aaa new-model</pre>	Enables AAA functionality.
Step 4	<p>aaa authentication login default group {tacacs+ radius}</p> <p>Example:</p> <pre>SwitchController(config)# aaa authentication login default group tacacs+</pre>	Defines the list of authentication methods at login.
Step 5	<p>aaa authorization auth-proxy default group {tacacs+ radius}</p> <p>Example:</p> <pre>SwitchController(config)# aaa authorization auth-proxy</pre>	Creates an authorization method list for web-based authorization.

	Command or Action	Purpose
	<code>default group tacacs+</code>	
Step 6	<p>tacacs-server host <i>{hostname ip_address}</i></p> <p>Example:</p> <pre>SwitchController(config)# tacacs-server host 10.1.1.1</pre>	Specifies an AAA server.
Step 7	<p>tacacs-server key <i>{key-data}</i></p> <p>Example:</p> <pre>SwitchController(config)# tacacs-server key</pre>	Configures the authorization and encryption key used between the switch and the TACACS server.
Step 8	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 9	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 10	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring Switch-to-RADIUS-Server Communication

Follow these steps to configure the RADIUS server parameters:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip radius source-interface vlan** *vlan interface number**interface_name*
4. **radius-server host** *{hostname | ip-address}* **test username** *username*
5. **radius-server key** *string*
6. **radius-server vsa send authentication** *string*
7. **radius-server dead-criteria tries** *num-tries*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>SwitchController> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 3	ip radius source-interface vlan <i>vlan interface number</i> <i>interface_name</i> Example: <pre>SwitchController(config)# ip radius source-interface vlan 80</pre>	Specifies that the RADIUS packets have the IP address of the indicated interface.
Step 4	radius-server host <i>{hostname ip-address}</i> test username <i>username</i> Example: <pre>SwitchController(config)# radius-server host 172.120.39.46 test username user1</pre>	<p>Specifies the host name or IP address of the remote RADIUS server.</p> <p>The test username <i>username</i> option enables automated testing of the RADIUS server connection. The specified <i>username</i> does not need to be a valid user name.</p> <p>The key option specifies an authentication and encryption key to use between the switch and the RADIUS server.</p> <p>To use multiple RADIUS servers, reenter this command for each server.</p>

	Command or Action	Purpose
Step 5	radius-server key <i>string</i> Example: SwitchController(config)# radius-server key rad123	Configures the authorization and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.
Step 6	radius-server vsa send authentication <i>string</i> Example: SwitchController(config)# radius-server vsa send authentication	Enable downloading of an ACL from the RADIUS server.
Step 7	radius-server dead-criteria tries <i>num-tries</i> Example: SwitchController(config)# radius-server dead-criteria tries 30	Specifies the number of unanswered sent messages to a RADIUS server before considering the server to be inactive. The range of <i>num-tries</i> is 1 to 100.
Step 8	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.

Configuring the HTTP Server

To use web-based authentication, you must enable the HTTP server within the SwitchController. You can enable the server for either HTTP or HTTPS.

Follow these steps to enable the server for either HTTP or HTTPS:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http secure-server**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	ip http server Example: SwitchController(config)# ip http server	Enables the HTTP server. The web-based authentication feature uses the HTTP server to communicate with the hosts for user authentication.
Step 4	ip http secure-server Example: SwitchController(config)# ip http secure-server	Enables HTTPS. You can configure custom authentication proxy web pages or specify a redirection URL for successful login. Note To ensure secure authentication when you enter the ip http secure-server command, the login page is always in HTTPS (secure HTTP) even if the user sends an HTTP request.
Step 5	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.

Customizing the Authentication Proxy Web Pages

You can configure web authentication to display four substitute HTML pages to the user in place of the SwitchController 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 SwitchController flash memory.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission proxy http login page file** *device:login-filename*
4. **ip admission proxy http success page file** *device:success-filename*
5. **ip admission proxy http failure page file** *device:fail-filename*
6. **ip admission proxy http login expired page file** *device:expired-filename*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	ip admission proxy http login page file <i>device:login-filename</i> Example: SwitchController(config)# ip admission proxy http login page file disk1:login.htm	Specifies the location in the SwitchController memory file system of the custom HTML file to use in place of the default login page. The <i>device:</i> is flash memory.
Step 4	ip admission proxy http success page file <i>device:success-filename</i> Example: SwitchController(config)# ip admission proxy http success page file disk1:success.htm	Specifies the location of the custom HTML file to use in place of the default login success page.

	Command or Action	Purpose
Step 5	<p>ip admission proxy http failure page file <i>device:fail-filename</i></p> <p>Example:</p> <pre>SwitchController(config)# ip admission proxy http fail page file disk1:fail.htm</pre>	Specifies the location of the custom HTML file to use in place of the default login failure page.
Step 6	<p>ip admission proxy http login expired page file <i>device:expired-filename</i></p> <p>Example:</p> <pre>SwitchController(config)# ip admission proxy http login expired page file disk1:expired.htm</pre>	Specifies the location of the custom HTML file to use in place of the default login expired page.
Step 7	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.

Related Topics

[Authentication Proxy Web Page Guidelines](#), on page 368

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission proxy http success redirect *url-string***
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	ip admission proxy http success redirect <i>url-string</i> Example: SwitchController(config)# ip admission proxy http success redirect www.example.com	Specifies a URL for redirection of the user in place of the default login success page.
Step 4	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.

Related Topics

[Redirection URL for Successful Login Guidelines, on page 369](#)

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission max-login-attempts *number***
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	ip admission max-login-attempts <i>number</i> Example: SwitchController (config)# ip admission max-login-attempts 10	Sets the maximum number of failed login attempts. The range is 1 to 2147483647 attempts. The default is 5.
Step 4	end Example: SwitchController (config)# end	Returns to privileged EXEC mode.
Step 5	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 6	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring a Web Authentication Local Banner

Follow these steps to configure a local banner on a switch that has web authentication configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission auth-proxy-banner http** [*banner-text* | *file-path*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	ip admission auth-proxy-banner http [<i>banner-text</i> <i>file-path</i>] Example: SwitchController(config)# ip admission auth-proxy-banner http C My Switch C	Enables the local banner. (Optional) Create a custom banner by entering <i>C banner-text C</i> (where <i>C</i> is a delimiting character), or <i>file-path</i> that indicates a file (for example, a logo or text file) that appears in the banner.
Step 4	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.
Step 5	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 6	copy running-config startup-config Example: SwitchController# copy running-config	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	<code>startup-config</code>	

Removing Web-Based Authentication Cache Entries

Follow these steps to remove web-based authentication cache entries:

SUMMARY STEPS

1. `enable`
2. `clear ip auth-proxy cache {* | host ip address}`
3. `clear ip admission cache {* | host ip address}`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example:</p> <pre>SwitchController> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p><code>clear ip auth-proxy cache {* host ip address}</code></p> <p>Example:</p> <pre>SwitchController# clear ip auth-proxy cache 192.168.4.5</pre>	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.
Step 3	<p><code>clear ip admission cache {* host ip address}</code></p> <p>Example:</p> <pre>SwitchController# clear ip admission cache 192.168.4.5</pre>	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.

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></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>
<UL>
  <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><OR><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>
<p>&nbsp;</p>

</center>
</BODY></HTML>
```

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 32: Privileged EXEC show Commands

Command	Purpose
show authentication sessions method webauth	Displays the web-based authentication settings for all interfaces for fastethernet, gigabitethernet, or tengigabitethernet
show authentication sessions interface <i>type slot/port[details]</i>	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.



CHAPTER 18

Configuring Port-Based Traffic Control

- [Finding Feature Information, page 390](#)
- [Information About Storm Control, page 390](#)
- [How to Configure Storm Control, page 392](#)
- [Monitoring Storm Control, page 397](#)
- [Where to Go Next, page 397](#)
- [Feature Information, page 397](#)
- [Information About Protected Ports, page 397](#)
- [How to Configure Protected Ports, page 398](#)
- [Monitoring Protected Ports, page 400](#)
- [Where to Go Next, page 400](#)
- [Feature Information, page 400](#)
- [Information About Port Blocking, page 400](#)
- [How to Configure Port Blocking, page 401](#)
- [Monitoring Port Blocking, page 403](#)
- [Where to Go Next, page 403](#)
- [Feature Information, page 403](#)
- [Prerequisites for Port Security, page 403](#)
- [Restrictions for Port Security, page 403](#)
- [Information About Port Security, page 404](#)
- [How to Configure Port Security, page 408](#)
- [Monitoring Port Security, page 417](#)
- [Configuration Examples for Port Security, page 417](#)
- [Where to Go Next, page 418](#)
- [Feature Information, page 418](#)

- [Information About Protocol Storm Protection, page 418](#)
- [How to Configure Protocol Storm Protection, page 419](#)
- [Monitoring Protocol Storm Protection, page 421](#)

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 Storm Control

Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm.

Storm control (or traffic suppression) monitors packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch counts the number of packets of a specified type received within the 1-second time interval and compares the measurement with a predefined suppression-level threshold.

How Traffic Activity is Measured

Storm control uses one of these methods to measure traffic activity:

- Bandwidth as a percentage of the total available bandwidth of the port that can be used by the broadcast, multicast, or unicast traffic
- Traffic rate in packets per second at which broadcast, multicast, or unicast packets are received
- Traffic rate in bits per second at which broadcast, multicast, or unicast packets are received
- Traffic rate in packets per second and for small frames. This feature is enabled globally. The threshold for small frames is configured for each interface.

With each method, the port blocks traffic when the rising threshold is reached. The port remains blocked until the traffic rate drops below the falling threshold (if one is specified) and then resumes normal forwarding. If the falling suppression level is not specified, the switch blocks all traffic until the traffic rate drops below the

rising suppression level. In general, the higher the level, the less effective the protection against broadcast storms.

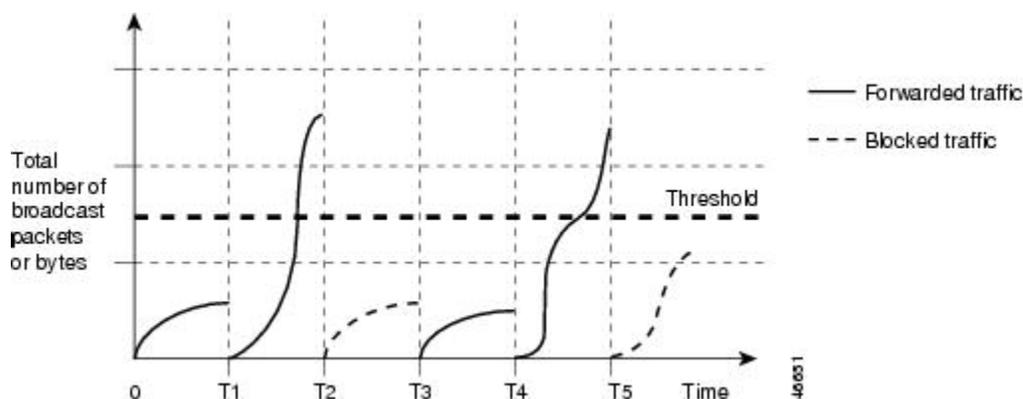
**Note**

When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked. However, the switch does not differentiate between routing updates, such as OSPF, and regular multicast data traffic, so both types of traffic are blocked.

Traffic Patterns

This example shows broadcast traffic patterns on an interface over a given period of time.

Figure 27: Broadcast Storm Control Example



Broadcast traffic being forwarded exceeded the configured threshold between time intervals T1 and T2 and between T4 and T5. When the amount of specified traffic exceeds the threshold, all traffic of that kind is dropped for the next time period. Therefore, broadcast traffic is blocked during the intervals following T2 and T5. At the next time interval (for example, T3), if broadcast traffic does not exceed the threshold, it is again forwarded.

The combination of the storm-control suppression level and the 1-second time interval controls the way the storm control algorithm works. A higher threshold allows more packets to pass through. A threshold value of 100 percent means that no limit is placed on the traffic. A value of 0.0 means that all broadcast, multicast, or unicast traffic on that port is blocked.

**Note**

Because packets do not arrive at uniform intervals, the 1-second time interval during which traffic activity is measured can affect the behavior of storm control.

You use the **storm-control** interface configuration commands to set the threshold value for each traffic type.

How to Configure Storm Control

Configuring Storm Control and Threshold Levels

You configure storm control on a port and enter the threshold level that you want to be used for a particular type of traffic.

However, because of hardware limitations and the way in which packets of different sizes are counted, threshold percentages are approximations. Depending on the sizes of the packets making up the incoming traffic, the actual enforced threshold might differ from the configured level by several percentage points.



Note

Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

Follow these steps to storm control and threshold levels:

Before You Begin

Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}
5. **storm-control action** {**shutdown** | **trap**}
6. **end**
7. **show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**]
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p>interface <i>interface-id</i></p> <p>Example:</p> <pre>SwitchController(config)# interface gigabitethernet1/0/1</pre>	Specifies the interface to be configured, and enter interface configuration mode.
Step 4	<p>storm-control {broadcast multicast unicast} level {<i>level</i> [<i>level-low</i>] bps <i>bps</i> [<i>bps-low</i>] pps <i>pps</i> [<i>pps-low</i>]}</p> <p>Example:</p> <pre>SwitchController(config-if)# storm-control unicast level 87 65</pre>	<p>Configures broadcast, multicast, or unicast storm control. By default, storm control is disabled.</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> • For <i>level</i>, specifies the rising threshold level for broadcast, multicast, or unicast traffic as a percentage (up to two decimal places) of the bandwidth. The port blocks traffic when the rising threshold is reached. The range is 0.00 to 100.00. • (Optional) For <i>level-low</i>, specifies the falling threshold level as a percentage (up to two decimal places) of the bandwidth. This value must be less than or equal to the rising suppression value. The port forwards traffic when traffic drops below this level. If you do not configure a falling suppression level, it is set to the rising suppression level. The range is 0.00 to 100.00. • If you set the threshold to the maximum value (100 percent), no limit is placed on the traffic. If you set the threshold to 0.0, all broadcast, multicast, and unicast traffic on that port is blocked. • For bps <i>bps</i>, specifies the rising threshold level for broadcast, multicast, or unicast traffic in bits per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0. • (Optional) For <i>bps-low</i>, specifies the falling threshold level in bits per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0. • For pps <i>pps</i>, specifies the rising threshold level for broadcast, multicast, or unicast traffic in packets per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0. • (Optional) For <i>pps-low</i>, specifies the falling threshold level in packets per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0.

	Command or Action	Purpose
		For BPS and PPS settings, you can use metric suffixes such as k, m, and g for large number thresholds.
Step 5	storm-control action {shutdown trap} Example: <pre>SwitchController(config-if)# storm-control action trap</pre>	Specifies the action to be taken when a storm is detected. The default is to filter out the traffic and not to send traps. <ul style="list-style-type: none"> • Select the shutdown keyword to error-disable the port during a storm. • Select the trap keyword to generate an SNMP trap when a storm is detected.
Step 6	end Example: <pre>SwitchController(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 7	show storm-control [interface-id] [broadcast multicast unicast] Example: <pre>SwitchController# show storm-control gigabitethernet1/0/1 unicast</pre>	Verifies the storm control suppression levels set on the interface for the specified traffic type. If you do not enter a traffic type, broadcast storm control settings are displayed.
Step 8	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring Small-Frame Arrival Rate

Incoming VLAN-tagged packets smaller than 67 bytes are considered small frames. They are forwarded by the switch, but they do not cause the switch storm-control counters to increment.

You globally enable the small-frame arrival feature on the switch and then configure the small-frame threshold for packets on each interface. Packets smaller than the minimum size and arriving at a specified rate (the threshold) are dropped since the port is error disabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **errdisable detect cause small-frame**
4. **errdisable recovery interval *interval***
5. **errdisable recovery cause small-frame**
6. **interface *interface-id***
7. **small-frame violation-rate *pps***
8. **end**
9. **show interfaces *interface-id***
10. **show running-config**
11. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	errdisable detect cause small-frame Example: SwitchController(config)# errdisable detect cause small-frame	Enables the small-frame rate-arrival feature on the switch.
Step 4	errdisable recovery interval <i>interval</i> Example: SwitchController(config)# errdisable recovery interval 60	(Optional) Specifies the time to recover from the specified error-disabled state.
Step 5	errdisable recovery cause small-frame Example: SwitchController(config)# errdisable recovery	(Optional) Configures the recovery time for error-disabled ports to be automatically re-enabled after they are error disabled by the arrival of small frames

	Command or Action	Purpose
	<code>cause small-frame</code>	Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.
Step 6	interface <i>interface-id</i> Example: <pre>SwitchController(config)# interface gigabitethernet1/0/2</pre>	Enters interface configuration mode, and specify the interface to be configured.
Step 7	small-frame violation-rate <i>pps</i> Example: <pre>SwitchController(config-if)# small-frame violation rate 10000</pre>	Configures the threshold rate for the interface to drop incoming packets and error disable the port. The range is 1 to 10,000 packets per second (pps)
Step 8	end Example: <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 9	show interfaces <i>interface-id</i> Example: <pre>SwitchController# show interfaces gigabitethernet1/0/2</pre>	Verifies the configuration.
Step 10	show running-config Example: <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 11	copy running-config startup-config Example: <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Monitoring Storm Control

Table 33: Commands for Displaying Storm Control Status and Configuration

Command	Purpose
show interfaces [<i>interface-id</i>] switchport	Displays the administrative and operational status of all switching (nonrouting) ports or the specified port, including port blocking and port protection settings.
show storm-control [<i>interface-id</i>] [broadcast multicast unicast]	Displays storm control suppression levels set on all interfaces or the specified interface for the specified traffic type or for broadcast traffic if no traffic type is entered.

Where to Go Next

.

Feature Information

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.

Information About Protected Ports

Protected Ports

Some applications require that no traffic be forwarded at Layer 2 between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor. In such an environment, the use of protected ports ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch.

Protected ports have these features:

- A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. Data traffic cannot be forwarded between protected ports at Layer 2; only control traffic, such as PIM packets, is forwarded because these packets are processed by the CPU and forwarded in software. All data traffic passing between protected ports must be forwarded through a Layer 3 device.
- Forwarding behavior between a protected port and a nonprotected port proceeds as usual.

Because a switch stack represents a single logical switch, Layer 2 traffic is not forwarded between any protected ports in the switch stack, whether they are on the same or different switches in the stack.

Default Protected Port Configuration

The default is to have no protected ports defined.

Protected Ports Guidelines

You can configure protected ports on a physical interface (for example, Gigabit Ethernet port 1) or an EtherChannel group (for example, port-channel 5). When you enable protected ports for a port channel, it is enabled for all ports in the port-channel group.

Do not configure a private-VLAN port as a protected port. Do not configure a protected port as a private-VLAN port. A private-VLAN isolated port does not forward traffic to other isolated ports or community ports.

How to Configure Protected Ports

Configuring a Protected Port

Before You Begin

Protected ports are not pre-defined. This is the task to configure one.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **switchport protected**
5. **end**
6. **show interfaces *interface-id* switchport**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>SwitchController> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet1/0/1	Specifies the interface to be configured, and enter interface configuration mode.
Step 4	switchport protected Example: SwitchController(config-if)# switchport protected	Configures the interface to be a protected port.
Step 5	end Example: SwitchController(config)# end	Returns to privileged EXEC mode.
Step 6	show interfaces <i>interface-id</i> switchport Example: SwitchController# show interfaces gigabitethernet1/0/1 switchport	Verifies your entries.
Step 7	show running-config Example: SwitchController# show running-config	Verifies your entries.
Step 8	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Monitoring Protected Ports

Table 34: Commands for Displaying Protected Port Settings

Command	Purpose
<code>show interfaces [interface-id] switchport</code>	Displays the administrative and operational status of all switching (nonrouting) ports or the specified port, including port blocking and port protection settings.

Where to Go Next

.

Feature Information

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.

Information About Port Blocking

Port Blocking

By default, the switch floods packets with unknown destination MAC addresses out of all ports. If unknown unicast and multicast traffic is forwarded to a protected port, there could be security issues. To prevent unknown unicast or multicast traffic from being forwarded from one port to another, you can block a port (protected or nonprotected) from flooding unknown unicast or multicast packets to other ports.



Note

With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.

How to Configure Port Blocking

Blocking Flooded Traffic on an Interface

Before You Begin

The interface can be a physical interface or an EtherChannel group. When you block multicast or unicast traffic for a port channel, it is blocked on all ports in the port-channel group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport block multicast**
5. **switchport block unicast**
6. **end**
7. **show interfaces** *interface-id* **switchport**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet1/0/1	Specifies the interface to be configured, and enter interface configuration mode.
Step 4	switchport block multicast	Blocks unknown multicast forwarding out of the port.

	Command or Action	Purpose
	<p>Example:</p> <pre>SwitchController(config-if)# switchport block multicast</pre>	<p>Note Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.</p>
Step 5	<p>switchport block unicast</p> <p>Example:</p> <pre>SwitchController(config-if)# switchport block unicast</pre>	Blocks unknown unicast forwarding out of the port.
Step 6	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 7	<p>show interfaces interface-id switchport</p> <p>Example:</p> <pre>SwitchController# show interfaces gigabitethernet1/0/1 switchport</pre>	Verifies your entries.
Step 8	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 9	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Monitoring Port Blocking

Table 35: Commands for Displaying Port Blocking Settings

Command	Purpose
<code>show interfaces [interface-id] switchport</code>	Displays the administrative and operational status of all switching (nonrouting) ports or the specified port, including port blocking and port protection settings.

Where to Go Next

.

Feature Information

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.

Prerequisites for Port Security



Note

If you try to set the maximum value to a number less than the number of secure addresses already configured on an interface, the command is rejected.

Restrictions for Port Security

The maximum number of secure MAC addresses that you can configure on a switch or switch stack is set by the maximum number of available MAC addresses allowed in the system. This number is determined by the active Switch Database Management (SDM) template. This number is the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.

Information About Port Security

Port Security

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.

If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs. Also, if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port, a violation is flagged.

Related Topics

[Enabling and Configuring Port Security, on page 408](#)

[Configuration Examples for Port Security, on page 417](#)

Types of Secure MAC Addresses

The switch supports these types of secure MAC addresses:

- Static secure MAC addresses—These are manually configured by using the **switchport port-security mac-address *mac-address*** interface configuration command, stored in the address table, and added to the switch running configuration.
- Dynamic secure MAC addresses—These are dynamically configured, stored only in the address table, and removed when the switch restarts.
- Sticky secure MAC addresses—These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, when the switch restarts, the interface does not need to dynamically reconfigure them.

Sticky Secure MAC Addresses

You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling sticky learning. The interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. All sticky secure MAC addresses are added to the running configuration.

The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the sticky secure MAC addresses in the configuration file, when the switch restarts, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost.

If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

Security Violations

It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.
- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

You can configure the interface for one of three violation modes, based on the action to be taken if a violation occurs:

- **protect**—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.



Note We do not recommend configuring the protect violation mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

- **restrict**—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. In this mode, you are notified that a security violation has occurred. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.
- **shutdown**—a port security violation causes the interface to become error-disabled and to shut down immediately, and the port LED turns off. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands. This is the default mode.
- **shutdown vlan**—Use to set the security violation mode per-VLAN. In this mode, the VLAN is error disabled instead of the entire port when a violation occurs

This table shows the violation mode and the actions taken when you configure an interface for port security.

Table 36: Security Violation Mode Actions

Violation Mode	Traffic is forwarded 12	Sends SNMP trap	Sends syslog message	Displays error message 13	Violation counter increments	Shuts down port
protect	No	No	No	No	No	No
restrict	No	Yes	Yes	No	Yes	No

Violation Mode	Traffic is forwarded 12	Sends SNMP trap	Sends syslog message	Displays error message 13	Violation counter increments	Shuts down port
shutdown	No	No	No	No	Yes	Yes
shutdown vlan	No	No	Yes	No	Yes	No 14

¹² Packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses.

¹³ The switch returns an error message if you manually configure an address that would cause a security violation.

¹⁴ Shuts down only the VLAN on which the violation occurred.

Port Security Aging

You can use port security aging to set the aging time for all secure addresses on a port. Two types of aging are supported per port:

- Absolute—The secure addresses on the port are deleted after the specified aging time.
- Inactivity—The secure addresses on the port are deleted only if the secure addresses are inactive for the specified aging time.

Related Topics

[Enabling and Configuring Port Security Aging](#), on page 413

Port Security and Switch Stacks

When a switch joins a stack, the new switch will get the configured secure addresses. All dynamic secure addresses are downloaded by the new stack member from the other stack members.

When a switch (either the active switch or a stack member) leaves the stack, the remaining stack members are notified, and the secure MAC addresses configured or learned by that switch are deleted from the secure MAC address table.

Default Port Security Configuration

Table 37: Default Port Security Configuration

Feature	Default Setting
Port security	Disabled on a port.
Sticky address learning	Disabled.

Feature	Default Setting
Maximum number of secure MAC addresses per port	1.
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Port security aging	Disabled. Aging time is 0. Static aging is disabled. Type is absolute.

Port Security Configuration Guidelines

- Port security can only be configured on static access ports or trunk ports. A secure port cannot be a dynamic access port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).



Note Voice VLAN is only supported on access ports and not on trunk ports, even though the configuration is allowed.

- A secure port cannot be a private-VLAN port.
- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the phone.
- When a trunk port configured with port security and assigned to an access VLAN for data traffic and to a voice VLAN for voice traffic, entering the **switchport voice** and **switchport priority extend** interface configuration commands has no effect.

When a connected device uses the same MAC address to request an IP address for the access VLAN and then an IP address for the voice VLAN, only the access VLAN is assigned an IP address.
- When you enter a maximum secure address value for an interface, and the new value is greater than the previous value, the new value overwrites the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.
- The switch does not support port security aging of sticky secure MAC addresses.

This table summarizes port security compatibility with other port-based features.

Table 38: Port Security Compatibility with Other Switch Features

Type of Port or Feature on Port	Compatible with Port Security
DTP ¹⁵ port ¹⁶	No
Trunk port	Yes
Dynamic-access port ¹⁷	No
Routed port	No
SPAN source port	Yes
SPAN destination port	No
EtherChannel	Yes
Tunneling port	Yes
Protected port	Yes
IEEE 802.1x port	Yes
Voice VLAN port ¹⁸	Yes
Private VLAN port	No
IP source guard	Yes
Dynamic Address Resolution Protocol (ARP) inspection	Yes
Flex Links	Yes

¹⁵ DTP=Dynamic Trunking Protocol

¹⁶ A port configured with the **switchport mode dynamic** interface configuration command.

¹⁷ A VLAN Query Protocol (VQP) port configured with the **switchport access vlan dynamic** interface configuration command.

¹⁸ You must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN.

How to Configure Port Security

Enabling and Configuring Port Security

Before You Begin

This task restricts input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport mode** {access | trunk}
5. **switchport voice vlan** *vlan-id*
6. **switchport port-security**
7. **switchport port-security** [maximum *value* [vlan {*vlan-list* | {access | voice}}]]
8. **switchport port-security violation** {protect | restrict | shutdown | shutdown vlan}
9. **switchport port-security** [mac-address *mac-address* [vlan {*vlan-id* | {access | voice}}]]
10. **switchport port-security mac-address sticky**
11. **switchport port-security mac-address sticky** [*mac-address* | vlan {*vlan-id* | {access | voice}}]
12. **end**
13. **show port-security**
14. **show running-config**
15. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 3	interface <i>interface-id</i> Example: SwitchController(config)# interface gigabitethernet1/0/1	Specifies the interface to be configured, and enter interface configuration mode.
Step 4	switchport mode {access trunk} Example: SwitchController(config-if)#	Sets the interface switchport mode as access or trunk; an interface in the default mode (dynamic auto) cannot be configured as a secure port.

	Command or Action	Purpose
	<code>switchport mode access</code>	
Step 5	<p>switchport voice vlan <i>vlan-id</i></p> <p>Example:</p> <pre>SwitchController(config-if) # switchport voice vlan 22</pre>	<p>Enables voice VLAN on a port.</p> <p><i>vlan-id</i>—Specifies the VLAN to be used for voice traffic.</p>
Step 6	<p>switchport port-security</p> <p>Example:</p> <pre>SwitchController(config-if) # switchport port-security</pre>	<p>Enable port security on the interface.</p>
Step 7	<p>switchport port-security [maximum value [vlan {<i>vlan-list</i> {access voice}}]]</p> <p>Example:</p> <pre>SwitchController(config-if) # switchport port-security maximum 20</pre>	<p>(Optional) Sets the maximum number of secure MAC addresses for the interface. The maximum number of secure MAC addresses that you can configure on a switch or switch stack is set by the maximum number of available MAC addresses allowed in the system. This number is set by the active Switch Database Management (SDM) template. This number is the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.</p> <p>(Optional) vlan—sets a per-VLAN maximum value</p> <p>Enter one of these options after you enter the vlan keyword:</p> <ul style="list-style-type: none"> • <i>vlan-list</i>—On a trunk port, you can set a per-VLAN maximum value on a range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used. • access—On an access port, specifies the VLAN as an access VLAN. • voice—On an access port, specifies the VLAN as a voice VLAN. <p>Note The voice keyword is available only if a voice VLAN is configured on a port and if that port is not the access VLAN. If an interface is configured for voice VLAN, configure a maximum of two secure MAC addresses.</p>
Step 8	<p>switchport port-security violation {protect restrict shutdown shutdown vlan}</p> <p>Example:</p> <pre>SwitchController(config-if) # switchport port-security violation restrict</pre>	<p>(Optional) Sets the violation mode, the action to be taken when a security violation is detected, as one of these:</p> <ul style="list-style-type: none"> • protect—When the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

	Command or Action	Purpose
		<p>Note We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.</p> <ul style="list-style-type: none"> • restrict—When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. • shutdown—The interface is error-disabled when a violation occurs, and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. • shutdown vlan—Use to set the security violation mode per VLAN. In this mode, the VLAN is error disabled instead of the entire port when a violation occurs. <p>Note When a secure port is in the error-disabled state, you can bring it out of this state by entering the errdisable recovery cause psecure-violation global configuration command. You can manually re-enable it by entering the shutdown and no shutdown interface configuration commands or by using the clear errdisable interface vlan privileged EXEC command.</p>
Step 9	<p>switchport port-security [mac-address mac-address [vlan {vlan-id} {access voice}]]</p> <p>Example:</p> <pre>SwitchController(config-if) # switchport port-security mac-address 00:A0:C7:12:C9:25 vlan 3 voice</pre>	<p>(Optional) Enters a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.</p> <p>Note If you enable sticky learning after you enter this command, the secure addresses that were dynamically learned are converted to sticky secure MAC addresses and are added to the running configuration.</p> <p>(Optional) vlan—sets a per-VLAN maximum value.</p> <p>Enter one of these options after you enter the vlan keyword:</p> <ul style="list-style-type: none"> • vlan-id—On a trunk port, you can specify the VLAN ID and the MAC address. If you do not specify a VLAN ID, the native VLAN is used. • access—On an access port, specifies the VLAN as an access VLAN. • voice—On an access port, specifies the VLAN as a voice VLAN. <p>Note The voice keyword is available only if a voice VLAN is configured on a port and if that port is not the access VLAN. If an interface is configured for voice VLAN, configure a maximum of two secure MAC addresses.</p>
Step 10	switchport port-security mac-address sticky	(Optional) Enables sticky learning on the interface.

	Command or Action	Purpose
	<p>Example:</p> <pre>SwitchController(config-if) # switchport port-security mac-address sticky</pre>	
Step 11	<p>switchport port-security mac-address sticky [<i>mac-address</i> vlan {<i>vlan-id</i> {access voice}}]</p> <p>Example:</p> <pre>SwitchController(config-if) # switchport port-security mac-address sticky 00:A0:C7:12:C9:25 vlan voice</pre>	<p>(Optional) Enters a sticky secure MAC address, repeating the command as many times as necessary. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned, are converted to sticky secure MAC addresses, and are added to the running configuration.</p> <p>Note If you do not enable sticky learning before this command is entered, an error message appears, and you cannot enter a sticky secure MAC address.</p> <p>(Optional) vlan—sets a per-VLAN maximum value.</p> <p>Enter one of these options after you enter the vlan keyword:</p> <ul style="list-style-type: none"> • vlan-id—On a trunk port, you can specify the VLAN ID and the MAC address. If you do not specify a VLAN ID, the native VLAN is used. • access—On an access port, specifies the VLAN as an access VLAN. • voice—On an access port, specifies the VLAN as a voice VLAN. <p>Note The voice keyword is available only if a voice VLAN is configured on a port and if that port is not the access VLAN.</p>
Step 12	<p>end</p> <p>Example:</p> <pre>SwitchController(config) # end</pre>	Returns to privileged EXEC mode.
Step 13	<p>show port-security</p> <p>Example:</p> <pre>SwitchController# show port-security</pre>	Verifies your entries.
Step 14	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 15	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy</pre>	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	<code>running-config startup-config</code>	

Related Topics

[Port Security, on page 369](#)

[Port Security, on page 404](#)

[Configuration Examples for Port Security, on page 417](#)

Enabling and Configuring Port Security Aging

Use this feature to remove and add devices on a secure port without manually deleting the existing secure MAC addresses and to still limit the number of secure addresses on a port. You can enable or disable the aging of secure addresses on a per-port basis.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `switchport port-security aging {static | time time | type {absolute | inactivity}}`
5. `end`
6. `show port-security [interface interface-id] [address]`
7. `show running-config`
8. `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example:</p> <pre>SwitchController> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	interface <i>interface-id</i> Example: <pre>SwitchController(config)# interface gigabitethernet1/0/1</pre>	Specifies the interface to be configured, and enter interface configuration mode.
Step 4	switchport port-security aging {static time <i>time</i> type {absolute inactivity}} Example: <pre>SwitchController(config-if)# switchport port-security aging time 120</pre>	<p>Enables or disable static aging for the secure port, or set the aging time or type.</p> <p>Note The switch does not support port security aging of sticky secure addresses.</p> <p>Enter static to enable aging for statically configured secure addresses on this port.</p> <p>For <i>time</i>, specifies the aging time for this port. The valid range is from 0 to 1440 minutes.</p> <p>For type, select one of these keywords:</p> <ul style="list-style-type: none"> • absolute—Sets the aging type as absolute aging. All the secure addresses on this port age out exactly after the time (minutes) specified lapses and are removed from the secure address list. • inactivity—Sets the aging type as inactivity aging. The secure addresses on this port age out only if there is no data traffic from the secure source addresses for the specified time period.
Step 5	end Example: <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 6	show port-security [interface <i>interface-id</i>] [address] Example: <pre>SwitchController# show port-security interface gigabitethernet1/0/1</pre>	Verifies your entries.
Step 7	show running-config Example: <pre>SwitchController# show running-config</pre>	Verifies your entries.

	Command or Action	Purpose
Step 8	copy running-config startup-config Example: SwitchController# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Related Topics

[Port Security Aging, on page 406](#)

Configuring Port Security and Private VLANs

Port security allows an administrator to limit the number of MAC addresses learned on a port or to define which MAC addresses can be learned on a port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **switchport mode private-vlan {host | promiscuous}**
5. **switchport port-security**
6. **end**
7. **show port-security [interface *interface-id*] [address]**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: SwitchController> enable	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p>interface <i>interface-id</i></p> <p>Example:</p> <pre>SwitchController(config)# interface gigabitethernet 1/0/8</pre>	Specifies the interface to be configured, and enter interface configuration mode.
Step 4	<p>switchport mode private-vlan {host promiscuous}</p> <p>Example:</p> <pre>SwitchController(config-if)# switchport mode private-vlan promiscuous</pre>	Enables a private vlan on the interface.
Step 5	<p>switchport port-security</p> <p>Example:</p> <pre>SwitchController(config-if)# switchport port-security</pre>	Enables port security on the interface.
Step 6	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 7	<p>show port-security [interface <i>interface-id</i>] [address]</p> <p>Example:</p> <pre>SwitchController# show port-security interface gigabitethernet1/0/8</pre>	Verifies your entries.
Step 8	<p>show running-config</p> <p>Example:</p> <pre>SwitchController# show running-config</pre>	Verifies your entries.
Step 9	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchController# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose

Monitoring Port Security

This table displays port security information.

Table 39: Commands for Displaying Port Security Status and Configuration

Command	Purpose
show port-security [<i>interface interface-id</i>]	Displays port security settings for the switch or for the specified interface, including the maximum allowed number of secure MAC addresses for each interface, the number of secure MAC addresses on the interface, the number of security violations that have occurred, and the violation mode.
show port-security [<i>interface interface-id</i>] address	Displays all secure MAC addresses configured on all switch interfaces or on a specified interface with aging information for each address.
show port-security interface <i>interface-id</i> vlan	Displays the number of secure MAC addresses configured per VLAN on the specified interface.

Configuration Examples for Port Security

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 50. The violation mode is the default, no static secure MAC addresses are configured, and sticky learning is enabled.

```
SwitchController(config)# interface gigabitethernet1/0/1
SwitchController(config-if)# switchport mode access
SwitchController(config-if)# switchport port-security
SwitchController(config-if)# switchport port-security maximum 50
SwitchController(config-if)# switchport port-security mac-address sticky
```

This example shows how to configure a static secure MAC address on VLAN 3 on a port:

```
SwitchController(config)# interface gigabitethernet1/0/2
SwitchController(config-if)# switchport mode trunk
SwitchController(config-if)# switchport port-security
SwitchController(config-if)# switchport port-security mac-address 0000.0200.0004 vlan 3
```

This example shows how to enable sticky port security on a port, to manually configure MAC addresses for data VLAN and voice VLAN, and to set the total maximum number of secure addresses to 20 (10 for data VLAN and 10 for voice VLAN).

```
SwitchController(config)# interface tengigabitethernet1/0/1
SwitchController(config-if)# switchport access vlan 21
SwitchController(config-if)# switchport mode access
SwitchController(config-if)# switchport voice vlan 22
SwitchController(config-if)# switchport port-security
SwitchController(config-if)# switchport port-security maximum 20
SwitchController(config-if)# switchport port-security violation restrict
SwitchController(config-if)# switchport port-security mac-address sticky
SwitchController(config-if)# switchport port-security mac-address sticky 0000.0000.0002
SwitchController(config-if)# switchport port-security mac-address 0000.0000.0003
SwitchController(config-if)# switchport port-security mac-address sticky 0000.0000.0001
vlan voice
SwitchController(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
SwitchController(config-if)# switchport port-security maximum 10 vlan access
SwitchController(config-if)# switchport port-security maximum 10 vlan voice
```

Related Topics

[Port Security, on page 404](#)

[Enabling and Configuring Port Security, on page 408](#)

Where to Go Next

.

Feature Information

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.

Information About Protocol Storm Protection

Protocol Storm Protection

When a switch is flooded with Address Resolution Protocol (ARP) or control packets, high CPU utilization can cause the CPU to overload. These issues can occur:

- Routing protocol can flap because the protocol control packets are not received, and neighboring adjacencies are dropped.
- Spanning Tree Protocol (STP) reconverges because the STP bridge protocol data unit (BPDU) cannot be sent or received.

- CLI is slow or unresponsive.

Using protocol storm protection, you can control the rate at which control packets are sent to the switch by specifying the upper threshold for the packet flow rate. The supported protocols are ARP, ARP snooping, Dynamic Host Configuration Protocol (DHCP) v4, DHCP snooping, Internet Group Management Protocol (IGMP), and IGMP snooping.

When the packet rate exceeds the defined threshold, the switch drops all traffic arriving on the specified virtual port for 30 seconds. The packet rate is measured again, and protocol storm protection is again applied if necessary.

For further protection, you can manually error disable the virtual port, blocking all incoming traffic on the virtual port. You can manually enable the virtual port or set a time interval for automatic re-enabling of the virtual port.

**Note**

Excess packets are dropped on no more than two virtual ports.

Virtual port error disabling is not supported for EtherChannel and Flexlink interfaces

Default Protocol Storm Protection Configuration

Protocol storm protection is disabled by default. When it is enabled, auto-recovery of the virtual port is disabled by default.

How to Configure Protocol Storm Protection

Enabling Protocol Storm Protection

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **psp {arp | dhcp | igmp} pps *value***
4. **errdisable detect cause psp**
5. **errdisable recovery interval *time***
6. **end**
7. **show psp config {arp | dhcp | igmp}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	<p>Example:</p> <pre>SwitchController> enable</pre>	
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 3	<p>psp {arp dhcp igmp} pps <i>value</i></p> <p>Example:</p> <pre>SwitchController(config)# psp dhcp pps 35</pre>	Configures protocol storm protection for ARP, IGMP, or DHCP. For <i>value</i> , specifies the threshold value for the number of packets per second. If the traffic exceeds this value, protocol storm protection is enforced. The range is from 5 to 50 packets per second.
Step 4	<p>errdisable detect cause psp</p> <p>Example:</p> <pre>SwitchController(config)# errdisable detect cause psp</pre>	(Optional) Enables error-disable detection for protocol storm protection. If this feature is enabled, the virtual port is error disabled. If this feature is disabled, the port drops excess packets without error disabling the port.
Step 5	<p>errdisable recovery interval <i>time</i></p> <p>Example:</p> <pre>SwitchController</pre>	(Optional) Configures an auto-recovery time (in seconds) for error-disabled virtual ports. When a virtual port is error-disabled, the switch auto-recovers after this time. The range is from 30 to 86400 seconds.
Step 6	<p>end</p> <p>Example:</p> <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode.
Step 7	<p>show psp config {arp dhcp igmp}</p> <p>Example:</p> <pre>SwitchController# show psp config dhcp</pre>	Verifies your entries.

Monitoring Protocol Storm Protection

Command	Purpose
<code>show psp config {arp dhcp igmp}</code>	Verify your entries.



Configuring Cisco TrustSec

- [Information about Cisco TrustSec, page 423](#)
- [Finding Feature Information, page 423](#)
- [Cisco TrustSec Features, page 424](#)
- [Feature Information for Cisco TrustSec, page 426](#)

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.

Finding Feature Information

To configure Cisco TrustSec on the switch, see the Cisco TrustSec Switch Configuration Guide at the following URL:

<http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec.html>

Release notes for Cisco TrustSec General Availability releases are at the following URL:

http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

Additional information about the Cisco TrustSec solution, including overviews, datasheets, features by platform matrix, and case studies, is available at the following URL:

<http://www.cisco.com/en/US/netsol/ns1051/index.html>

Cisco TrustSec Features

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.

Cisco TrustSec Feature	Description
802.1AE Tagging (MACsec)	<p>Protocol for IEEE 802.1AE-based wire-rate hop-to-hop Layer 2 encryption.</p> <p>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.</p> <p>This feature is only available between TrustSec hardware-capable devices.</p>
Endpoint Admission Control (EAC)	<p>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).</p>
Network Device Admission Control (NDAC)	<p>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.</p>
Security Group Access Control List (SGACL)	<p>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.</p>
Security Association Protocol (SAP)	<p>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.</p>

Cisco TrustSec Feature	Description
Security Group Tag (SGT)	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.
SGT Exchange Protocol (SXP) ¹⁹	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.

¹⁹ including SXPv2 in the context of Cisco TrustSec MACsec

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

Feature Information for Cisco TrustSec

Table 40: Feature Information for Cisco TrustSec

Feature Name	Release	Feature Information
<ul style="list-style-type: none"> • NDAC • SXPv1, SXPv2 • SGT • SGACL Layer2 Enforcement • Interface to SGT and VLAN to SGT mapping. • Subnet to SGT mapping • Layer 3 Port Mapping (PM) • Layer 3 Identity Port Mapping (IPM) • Security Group Name Download • SXP Loop Detection • Policy-based CoA 	Cisco IOS XE 3.3SE	These features were introduced on the Catalyst 3850 and 3650 switches and the Cisco 5700 Series Wireless LAN Controllers.
SXPv1 and SXPv2	Cisco IOS XE 15.0(2)EX	SXP is introduced on the Catalyst 2960-X switch.
SXPv1 and SXPv2	Cisco IOS XE 15.0(2)EX1	SXP is introduced on the Catalyst 2960-XR switch.



Configuring IPv6 First Hop Security

- [Finding Feature Information, page 427](#)
- [Prerequisites for First Hop Security in IPv6, page 427](#)
- [Restrictions for First Hop Security in IPv6, page 428](#)
- [Information about First Hop Security in IPv6, page 428](#)
- [How to Configure an IPv6 Snooping Policy, page 432](#)
- [How to Configure the IPv6 Binding Table Content , page 437](#)
- [How to Configure an IPv6 Neighbor Discovery Inspection Policy, page 439](#)
- [How to Configure an IPv6 Router Advertisement Guard Policy, page 444](#)
- [How to Configure an IPv6 DHCP Guard Policy , page 450](#)
- [Additional References, page 455](#)

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 First Hop Security in IPv6

- You have configured the necessary IPv6 enabled SDM template.
- You should be familiar with the IPv6 neighbor discovery feature.

Restrictions for First Hop Security in IPv6

- Although visible in the command-line help strings, the IPv6 first hop security (FHS) is not supported on the Catalyst 3750-G and 3750v2 switches. The command-line help strings are visible on these switches to support the FHS feature in a mixed switch stack scenario where one of these switches could become a master.
- The following restrictions apply when applying FHS policies to EtherChannel interfaces (Port Channels):
 - A physical port with an FHS policy attached cannot join an EtherChannel group.
 - An FHS policy cannot be attached to a physical port when it is a member of an EtherChannel group.

Information about First Hop Security in IPv6

First Hop Security in IPv6 (FHS IPv6) is a set of IPv6 security features, the policies of which can be attached to a physical interface, or a VLAN. An IPv6 software policy database service stores and accesses these policies. When a policy is configured or modified, the attributes of the policy are stored or updated in the software policy database, then applied as was specified. The following IPv6 policies are currently supported:

- IPv6 Snooping Policy—IPv6 Snooping Policy acts as a container policy that enables most of the features available with FHS in IPv6.
- IPv6 FHS Binding Table Content—A database table of IPv6 neighbors connected to the switch is created from information sources such as Neighbor Discovery (ND) protocol snooping. This database, or binding, table is used by various IPv6 guard features (such as IPv6 ND Inspection) to validate the link-layer address (LLA), the IPv4 or IPv6 address, and prefix binding of the neighbors to prevent spoofing and redirect attacks.
- NDP Address Gleaning—The NDP address gleaning feature is enabled by default when you configure the **ipv6 snooping policy** global configuration command. To disable this function, enter the **no protocol ndp global** configuration command and attach the policy to the target port or VLAN.
- IPv6 DHCP Address Gleaning—The IPv6 DHCP address gleaning feature provides the ability to extract addresses from DHCP messages and populate the binding table. The switch extracts address binding information from the following types of DHCPv6 exchanges (using User Datagram Protocol (UDP), ports 546 and 547):
 - DHCP-REQUEST
 - DHCP-CONFIRM
 - DHCP-RENEW
 - DHCP-REBIND
 - DHCP-REPLY
 - DHCP-RELEASE
 - DHCP-DECLINE

After a switch receives a DHCP-REQUEST message from a client, one of the following can happen:

- The switch receives a DHCP-REPLY message from the DHCP server and a binding table entry is created in the REACHABLE state and completed. The reply contains the IP address and the MAC address in the Layer 2 DMAC field.

Creating an entry in the binding table allows the switch to learn addresses assigned by DHCP. A binding table can have one of the following states:

- INCOMPLETE—Address resolution is in progress and the link-layer address is not yet known.
 - REACHABLE—The table is known to be reachable within the last reachable time interval.
 - STALE—The table requires re-resolution.
 - SEARCH—The feature creating the entry does not have the Layer 2 address and requests the binding table to search for the Layer 2 address.
 - VERIFY—The Layer 2 and Layer 3 addresses are known and a duplicate address detection (DAD) Neighbor solicitation (NS) unicast message is sent to the Layer 2 and Layer 3 destinations to verify the addresses.
 - DOWN—The interface from which the entry was learned is down, preventing verification.
- The DHCP server sends a DHCP-DECLINE or DHCP release message and the entry is deleted.
 - The client sends a DHCP-RENEW message to the server that allocates the address or a DHCP-REBIND message to any server and the lifespan of the entry is extended.
 - The server does not reply and the session is timed-out.

To enable this feature, configure a policy using the `ipv6 snooping policy policy-name global` configuration command.

You can configure a policy and attach it to a DHCP guard to prevent the binding table from being filled with forged DHCP messages.

- IPv6 Neighbor Discovery Inspection—IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables. IPv6 ND inspection analyzes neighbor discovery messages in order to build a trusted binding table database and IPv6 neighbor discovery messages that do not conform are dropped. An ND message is considered trustworthy if its IPv6-to-Media Access Control (MAC) mapping is verifiable.

This feature mitigates some of the inherent vulnerabilities of the ND mechanism, such as attacks on DAD, address resolution, router discovery, and the neighbor cache.

For detailed information about IPv6 Neighbor Discovery Inspection, see the [“IPv6 Neighbor Discovery Inspection”](#) chapter of the Cisco IOS IPv6 Configuration Guide Library on Cisco.com.

- IPv6 Binding Table Recovery Mechanism—The IPv6 first-hop security binding table recovery feature recovers the missing binding table entries when the resolution for a destination address fails in the destination guard. Upon a failure, a binding table entry is recovered by querying the DHCP server or the destination host depending on the configuration.

The recovery mechanism blocks any data traffic sourced from an unknown source, that is, a source not already specified in the binding table and previously learned by using NDP or Dynamic Host Configuration Protocol (DHCP) gleaning.

For detailed information about IPv6 binding table recovery, see the [“IPv6 First-Hop Security Binding Table”](#) chapter of the Cisco IOS IPv6 Configuration Guide Library on Cisco.com.

- IPv6 Data Address Gleaning—The IPv6 data address gleaning feature provides the ability to extract addresses from redirected datatracffic, to discover neighbors, and to populate binding tables.

When a port receives a data packet where the binding is unknown, that is, the neighbor is in an INCOMPLETE state and the link-layer address is not yet known, the switch sends a DAD NS NDP unicast message to the port from which the data packet was received.

After the host replies with a DAD Neighbor Advertisement (NA) NDP message, the binding table is updated and a private VLAN ACL (PVACL) is installed in the hardware for this binding.

If the host does not reply with a DAD NA, after the binding table timer expires, the hardware is notified and any resources associated with that binding are released.

To enable this feature, configure a policy with **data-glean** and attach the policy to a target port. To debug the policy, use the **debug ipv6 snooping** privileged EXEC command.

- IPv6 Router Advertisement Guard—The IPv6 Router Advertisement (RA) guard feature enables the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network switch platform. RAs are used by routers to announce themselves on the link. The RA Guard feature analyzes the RAs and filters out bogus RAs sent by unauthorized routers. In host mode, all router advertisement and router redirect messages are disallowed on the port. The RA guard feature compares configuration information on the Layer 2 device with the information found in the received RA frame. Once the Layer 2 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.

For detailed information about IPv6 Router Advertisement Guard, see the [“IPv6 Router Advertisement Guard”](#) chapter of the Cisco IOS IPv6 Configuration Guide Library on Cisco.com.

- IPv6 Device Tracking—The IPv6 device tracking feature provides IPv6 host liveness tracking so that a neighbor table can be updated when an IPv6 host disappears. The feature tracks the liveness of the neighbors connected through the Layer 2 switch on regular basis in order to revoke network access privileges as they become inactive.

For detailed information about IPv6 Device Tracking, see the [“IPv6 Device Tracking”](#) chapter of the Cisco IOS IPv6 Configuration Guide Library on Cisco.com.

- IPv6 DHCP Guard—The IPv6 DHCP Guard feature blocks reply and advertisement messages that come from unauthorized DHCPv6 servers and relay agents. IPv6 DHCP guard can prevent forged messages from being entered in the binding table and block DHCPv6 server messages when they are received on ports that are not explicitly configured as facing a DHCPv6 server or DHCP relay. To use this feature, configure a policy and attach it to an interface or a VLAN. To debug DHCP guard packets, use the **debug ipv6 snooping dhcp-guard** privileged EXEC command.

- IPv6 Port-Based Access List Support—The IPv6 port-based access list (PACL) feature provides the ability to provide access control (permit or deny) on Layer 2 switch ports for IPv6 traffic. IPv6 PACLs are similar to IPv4 PACLs, which provide access control on Layer 2 switch ports for IPv4 traffic.

With Catalyst 3750-E, 3750X, 3560E, 3560-X, 3750v2, and 3560 v2 switches, this feature is supported in hardware and only in ingress direction. In a mixed stack scenario where the stack has a switch that does not support IPv6 FHS, the VLAN target is disabled on the whole switch for security. Port targets are allowed on the IPv6 FHS-capable ports of the switch. If a non-supporting switch becomes the stack master, the IPv6 FHS functions are still supported on the IPv6 FHS-capable ports of the switch.

Access lists determine which traffic is blocked and which traffic is forwarded at switch interfaces and allow filtering based on source and destination addresses, inbound and outbound, to a specific interface. Each access list has an implicit deny statement at the end. To configure an IPv6 PACL, you have to create an IPv6 access list and then configure the PACL mode on the specified IPv6 Layer 2 interface.

PACL can filter ingress traffic on Layer 2 interfaces based on Layer 3 and Layer 4 header information or non-IP Layer 2 information.

- IPv6 Source Guard—Like IPv4 Source Guard, IPv6 Source Guard validates the source address or prefix to prevent source address spoofing.

A source guard programs the hardware to allow or deny traffic based on source or destination addresses. It deals exclusively with data packet traffic.

The IPv6 source guard feature provides the ability to use the IPv6 binding table to install PACLs to prevent a host from sending packets with an invalid IPv6 source address.

To debug source-guard packets, use the `debug ipv6 snooping source-guard` privileged EXEC command.



Note The IPv6 PACL feature is supported only in the ingress direction; it is not supported in the egress direction.

The following restrictions apply:

- An FHS policy cannot be attached to a physical port when it is a member of an EtherChannel group.
- When IPv6 source guard is enabled on a switch port, NDP or DHCP snooping must be enabled on the interface to which the switch port belongs. Otherwise, all data traffic from this port will be blocked.
- An IPv6 source guard policy cannot be attached to a VLAN. It is supported only at the interface level.
- You cannot use IPv6 Source Guard and Prefix Guard together. When you attach the policy to an interface, it should be "validate address" or "validate prefix" but not both.
- PVLAN and Source/Prefix Guard cannot be applied together.

For more information on IPv6 Source Guard, see the [IPv6 Source Guard](#) chapter of the Cisco IOS IPv6 Configuration Guide Library on Cisco.com.

- IPv6 Prefix Guard—The IPv6 prefix guard feature works within the IPv6 source guard feature, to enable the device to deny traffic originated from non-topologically correct addresses. IPv6 prefix guard is often used when IPv6 prefixes are delegated to devices (for example, home gateways) using DHCP prefix delegation. The feature discovers ranges of addresses assigned to the link and blocks any traffic sourced with an address outside this range.

For more information on IPv6 Prefix Guard, see the [IPv6 Prefix Guard](#) chapter of the Cisco IOS IPv6 Configuration Guide Library on Cisco.com.

- IPv6 Destination Guard—The IPv6 destination guard feature works with IPv6 neighbor discovery to ensure that the device performs address resolution only for those addresses that are known to be active on the link. It relies on the address glean functionality to populate all destinations active on the link into the binding table and then blocks resolutions before they happen when the destination is not found in the binding table.



Note IPv6 Destination Guard is recommended only on Layer 3. It is not recommended on Layer2.

For more information about IPv6 Destination Guard, see the [IPv6 Destination Guard](#) chapter of the Cisco IOS IPv6 Configuration Guide Library on Cisco.com.

- IPv6 Neighbor Discovery Multicast Suppress—The IPv6 Neighbor Discovery multicast suppress feature is an IPv6 snooping feature that runs on a switch or a wireless controller and is used to reduce the amount of control traffic necessary for proper link operations.
- DHCPv6 Relay—Lightweight DHCPv6 Relay Agent—The DHCPv6 Relay—Lightweight DHCPv6 Relay Agent feature allows relay agent information to be inserted by an access node that performs a link-layer bridging (non-routing) function. Lightweight DHCPv6 Relay Agent (LDRA) functionality can be implemented in existing access nodes, such as DSL access multiplexers (DSLAMs) and Ethernet switches, that do not support IPv6 control or routing functions. LDRA is used to insert relay-agent options in DHCP version 6 (DHCPv6) message exchanges primarily to identify client-facing interfaces. LDRA functionality can be enabled on an interface and on a VLAN.

For more information about DHCPv6 Relay, See the [DHCPv6 Relay—Lightweight DHCPv6 Relay Agent](#) section of the IP Addressing: DHCP Configuration Guide, Cisco IOS Release 15.1SG.

How to Configure an IPv6 Snooping Policy

Beginning in privileged EXEC mode, follow these steps to configure IPv6 Snooping Policy :

SUMMARY STEPS

1. **configure terminal**
2. **ipv6 snooping policy *policy-name***
3. **{[default] | [device-role {node | switch}] | [limit address-count *value*] | [no] | [protocol {dhcp | ndp}] | [security-level {glean | guard | inspect}] | [tracking {disable [stale-lifetime [*seconds*] | infinite] | enable [reachable-lifetime [*seconds*] | infinite]}] | [trusted-port] }**
4. **end**
5. **show ipv6 snooping policy *policy-name***

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	<p>ipv6 snooping policy <i>policy-name</i></p> <p>Example: SwitchController(config)# ipv6 snooping policy example_policy</p>	Creates a snooping policy and enters IPv6 Snooping Policy Configuration mode.
Step 3	<p>[[default] [device-role {node switch}] [limit address-count value] [no] [protocol {dhcp ndp}] [security-level {glean guard inspect}] [tracking {disable [stale-lifetime [seconds infinite] enable [reachable-lifetime [seconds infinite] }] [trusted-port] }</p> <p>Example: SwitchController(config-ipv6-snooping)# security-level inspect</p> <p>Example: SwitchController(config-ipv6-snooping)# trusted-port</p>	<p>Enables data address gleaning, validates messages against various criteria, specifies the security level for messages.</p> <ul style="list-style-type: none"> • (Optional) default—Sets all to default options. • (Optional) device-role {node switch}—Specifies the role of the device attached to the port. Default is node. • (Optional) limit address-count value—Limits the number of addresses allowed per target. • (Optional) no—Negates a command or sets it to defaults. • (Optional) protocol {dhcp ndp}—Specifies which protocol should be redirected to the snooping feature for analysis. The default, is dhcp and ndp. To change the default, use the no protocol command. • (Optional) security-level {glean guard inspect}—Specifies the level of security enforced by the feature. Default is guard. <ul style="list-style-type: none"> glean—Gleans addresses from messages and populates the binding table without any verification. guard—Gleans addresses and inspects messages. In addition, it rejects RA and DHCP server messages. This is the default option. inspect—Gleans addresses, validates messages for consistency and conformance, and enforces address ownership. • (Optional) tracking {disable enable}—Overrides the default tracking behavior and specifies a tracking option. • (Optional) trusted-port—Sets up a trusted port. It disables the guard on applicable targets. Bindings learned through a trusted port have preference over bindings learned through any other port. A trusted port is given preference in case of a collision while making an entry in the table.
Step 4	<p>end</p> <p>Example: SwitchController(config-ipv6-snooping)# exit</p>	Exits configuration modes to Privileged EXEC mode.
Step 5	<p>show ipv6 snooping policy <i>policy-name</i></p> <p>Example: SwitchController#show ipv6 snooping policy example_policy</p>	Displays the snooping policy configuration.

What to Do Next

Attach an IPv6 Snooping policy to interfaces or VLANs.

How to Attach an IPv6 Snooping Policy to an Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Snooping policy on an interface or VLAN:

SUMMARY STEPS

1. **configure terminal**
2. **interface** *Interface_type stack/module/port*
3. **switchport**
4. **ipv6 snooping** [**attach-policy** *policy_name* [**vlan** {*vlan_id* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids*}] | **vlan** {*vlan_id* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
5. **do show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface <i>Interface_type stack/module/port</i> Example: SwitchController(config)# interface gigabitethernet 1/1/4	Specifies an interface type and identifier; enters the interface configuration mode.
Step 3	switchport Example: SwitchController(config-if)# switchport	Enters the Switchport mode. Note To configure Layer 2 parameters, if the interface is in Layer 3 mode, you must enter the switchport interface configuration command without any parameters to put the interface into Layer 2 mode. This shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 3 mode into Layer 2 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration. The command prompt displays as (config-if)# in Switchport configuration mode.

	Command or Action	Purpose
Step 4	<p>ipv6 snooping [attach-policy <i>policy_name</i> [vlan {<i>vlan_id</i> add <i>vlan_ids</i> except<i>vlan_ids</i> none remove <i>vlan_ids</i>}] vlan {<i>vlan_id</i> add <i>vlan_ids</i> except<i>vlan_ids</i> none remove <i>vlan_ids</i> all}]</p> <p>Example: SwitchController(config-if)# ipv6 snooping or SwitchController(config-if)# ipv6 snooping attach-policy example_policy or SwitchController(config-if)# ipv6 snooping vlan 111,112 or SwitchController(config-if)# ipv6 snooping attach-policy example_policy vlan 111,112</p>	<p>Attaches a custom ipv6 snooping policy to the interface or the specified VLANs on the interface. To attach the default policy to the interface, use the ipv6 snooping command without the attach-policy keyword. To attach the default policy to VLANs on the interface, use the ipv6 snooping vlan command. The default policy is, security-level guard, device-role node, protocol ndp and dhcp.</p>
Step 5	<p>do show running-config</p> <p>Example: SwitchController#(config-if)# do show running-config</p>	<p>Verifies that the policy is attached to the specified interface without exiting the interface configuration mode.</p>

How to Attach an IPv6 Snooping Policy to a Layer 2 EtherChannel Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Snooping policy on an EtherChannel interface or VLAN:

SUMMARY STEPS

1. **configure terminal**
2. **interface range** *Interface_name*
3. **ipv6 snooping** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
4. **do show running-config interface***portchannel_interface_name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface range <i>Interface_name</i> Example: SwitchController(config)# interface Po11	Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode. Tip Enter the do show interfaces summary command for quick reference to interface names and types.
Step 3	ipv6 snooping [attach-policy <i>policy_name</i> [vlan { <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }] vlan [{ <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }]] Example: SwitchController(config-if-range)# ipv6 snooping attach-policy example_policy or SwitchController(config-if-range)# ipv6 snooping attach-policy example_policy vlan 222,223,224 or SwitchController(config-if-range)# ipv6 snooping vlan 222, 223,224	Attaches the IPv6 Snooping policy to the interface or the specified VLANs on that interface. The default policy is attached if the attach-policy option is not used.
Step 4	do show running-config interface <i>portchannel_interface_name</i> Example: SwitchController#(config-if-range)# do show running-config int po11	Confirms that the policy is attached to the specified interface without exiting the configuration mode.

How to Attach an IPv6 Snooping Policy to VLANs Globally

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Snooping Policy to VLANs across multiple interfaces:

SUMMARY STEPS

1. **configure terminal**
2. **vlan configuration** *vlan_list*
3. **ipv6 snooping** [**attach-policy** *policy_name*]
4. **do show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	vlan configuration <i>vlan_list</i> Example: SwitchController(config)# vlan configuration 333	Specifies the VLANs to which the IPv6 Snooping policy will be attached ; enters the VLAN interface configuration mode.
Step 3	ipv6 snooping [attach-policy <i>policy_name</i>] Example: SwitchController(config-vlan-config)# ipv6 snooping attach-policy example_policy	Attaches the IPv6 Snooping policy to the specified VLANs across all switch and stack interfaces. The default policy is attached if the attach-policy option is not used. The default policy is, security-level guard , device-role node , protocol ndp and dhcp .
Step 4	do show running-config Example: SwitchController#(config-if)# do show running-config	Verifies that the policy is attached to the specified VLANs without exiting the interface configuration mode.

How to Configure the IPv6 Binding Table Content

Beginning in privileged EXEC mode, follow these steps to configure IPv6 Binding Table Content :

	Command or Action	Purpose
Step 6	show ipv6 neighbor binding Example: SwitchController# <code>show ipv6 neighbor binding</code>	Displays contents of a binding table.

How to Configure an IPv6 Neighbor Discovery Inspection Policy

Beginning in privileged EXEC mode, follow these steps to configure an IPv6 ND Inspection Policy:

SUMMARY STEPS

1. **configure terminal**
2. **[no]ipv6 nd inspection policy *policy-name***
3. **device-role {host | monitor | router | switch}**
4. **drop-unsecure**
5. **limit address-count *value***
6. **sec-level minimum *value***
7. **tracking {enable [reachable-lifetime {*value* | infinite}] | disable [stale-lifetime {*value* | infinite}]}**
8. **trusted-port**
9. **validate source-mac**
10. **no {device-role | drop-unsecure | limit address-count | sec-level minimum | tracking | trusted-port | validate source-mac}**
11. **default {device-role | drop-unsecure | limit address-count | sec-level minimum | tracking | trusted-port | validate source-mac}**
12. **do show ipv6 nd inspection policy *policy_name***

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# <code>configure terminal</code>	Enters the global configuration mode.
Step 2	[no]ipv6 nd inspection policy <i>policy-name</i> Example: SwitchController(config)# <code>ipv6 nd inspection policy example_policy</code>	Specifies the ND inspection policy name and enters ND Inspection Policy configuration mode.

	Command or Action	Purpose
Step 3	device-role { host monitor router switch } Example: SwitchController (config-nd-inspection) # device-role switch	Specifies the role of the device attached to the port. The default is host .
Step 4	drop-unsecure Example: SwitchController (config-nd-inspection) # drop-unsecure	Drops messages with no or invalid options or an invalid signature.
Step 5	limit address-count <i>value</i> Example: SwitchController (config-nd-inspection) # limit address-count 1000	Enter 1–10,000.
Step 6	sec-level minimum <i>value</i> Example: SwitchController (config-nd-inspection) # limit address-count 1000	Specifies the minimum security level parameter value when Cryptographically Generated Address (CGA) options are used.
Step 7	tracking { enable [reachable-lifetime { <i>value</i> infinite }] disable [stale-lifetime { <i>value</i> infinite }]} Example: SwitchController (config-nd-inspection) # tracking disable stale-lifetime infinite	Overrides the default tracking policy on a port.
Step 8	trusted-port Example: SwitchController (config-nd-inspection) # trusted-port	Configures a port to become a trusted port.
Step 9	validate source-mac Example: SwitchController (config-nd-inspection) # validate source-mac	Checks the source media access control (MAC) address against the link-layer address.
Step 10	no { device-role drop-unsecure limit address-count sec-level minimum tracking trusted-port validate source-mac } Example: SwitchController (config-nd-inspection) # no validate source-mac	Remove the current configuration of a parameter with the no form of the command.
Step 11	default { device-role drop-unsecure limit address-count sec-level minimum tracking trusted-port validate source-mac } Example: SwitchController (config-nd-inspection) # default limit address-count	Restores configuration to the default values.

	Command or Action	Purpose
Step 12	do show ipv6 nd inspection policy <i>policy_name</i> Example: SwitchController(config-nd-inspection)# do show ipv6 nd inspection policy example_policy	Verifies the ND Inspection Configuration without exiting ND inspection configuration mode.

How to Attach an IPv6 Neighbor Discovery Inspection Policy to an Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 ND Inspection policy to an interface or VLANs on an interface :

SUMMARY STEPS

1. **configure terminal**
2. **interface** *Interface_type stack/module/port*
3. **ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]]
4. **do show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface <i>Interface_type stack/module/port</i> Example: SwitchController(config)# interface gigabitethernet 1/1/4	Specifies an interface type and identifier; enters the interface configuration mode.
Step 3	ipv6 nd inspection [attach-policy <i>policy_name</i> [vlan { <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }] vlan [{ <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }]] Example: SwitchController(config-if)# ipv6 nd inspection attach-policy example_policy or SwitchController(config-if)# ipv6 nd inspection	Attaches the Neighbor Discovery Inspection policy to the interface or the specified VLANs on that interface. The default policy is attached if the attach-policy option is not used.

	Command or Action	Purpose
	<pre>attach-policy example_policy vlan 222,223,224</pre> <p>or</p> <pre>SwitchController(config-if)# ipv6 nd inspection vlan 222, 223,224</pre>	
Step 4	<p>do show running-config</p> <p>Example:</p> <pre>SwitchController#(config-if)# do show running-config</pre>	Verifies that the policy is attached to the specified interface without exiting the interface configuration mode.

How to Attach an IPv6 Neighbor Discovery Inspection Policy to a Layer 2 EtherChannel Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Neighbor Discovery Inspection policy on an EtherChannel interface or VLAN:

SUMMARY STEPS

1. **configure terminal**
2. **interface range** *Interface_name*
3. **ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]]
4. **do show running-config interfaceportchannel_interface_name**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.
Step 2	<p>interface range <i>Interface_name</i></p> <p>Example:</p> <pre>SwitchController(config)# interface Po11</pre>	Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode. Tip Enter the do show interfaces summary command for quick reference to interface names and types.

	Command or Action	Purpose
Step 3	<pre> ipv6 nd inspection [attach-policy <i>policy_name</i> [vlan {<i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }] vlan [{<i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }] Example: SwitchController(config-if-range)# ipv6 nd inspection attach-policy example_policy or SwitchController(config-if-range)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224 or SwitchController(config-if-range)#ipv6 nd inspection vlan 222, 223,224 </pre>	Attaches the ND Inspection policy to the interface or the specified VLANs on that interface. The default policy is attached if the attach-policy option is not used.
Step 4	<pre> do show running-config interface<i>portchannel_interface_name</i> Example: SwitchController#(config-if-range)# do show running-config int poll </pre>	Confirms that the policy is attached to the specified interface without exiting the configuration mode.

How to Attach an IPv6 Neighbor Discovery Inspection Policy to VLANs Globally

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 ND Inspection policy to VLANs across multiple interfaces:

SUMMARY STEPS

1. **configure terminal**
2. **vlan configuration** *vlan_list*
3. **ipv6 nd inspection** [*attach-policy policy_name*]
4. **do show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre> configure terminal Example: SwitchController# configure terminal </pre>	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	vlan configuration <i>vlan_list</i> Example: SwitchController(config)# vlan configuration 334	Specifies the VLANs to which the IPv6 Snooping policy will be attached ; enters the VLAN interface configuration mode.
Step 3	ipv6 nd inspection [attach-policy <i>policy_name</i>] Example: SwitchController (config-vlan-config)# ipv6 nd inspection attach-policy example_policy	<p>Attaches the IPv6 Neighbor Discovery policy to the specified VLANs across all switch and stack interfaces. The default policy is attached if the attach-policy option is not used.</p> <p>The default policy is, device-role host, no drop-unsecure, limit address-count disabled, sec-level minimum is disabled, tracking is disabled, no trusted-port, no validate source-mac.</p>
Step 4	do show running-config Example: SwitchController#(config-if)# do show running-config	Confirms that the policy is attached to the specified VLANs without exiting the configuration mode.

How to Configure an IPv6 Router Advertisement Guard Policy

Beginning in privileged EXEC mode, follow these steps to configure an IPv6 Router Advertisement policy :

SUMMARY STEPS

1. **configure terminal**
2. **[no]ipv6 nd rguard policy** *policy-name*
3. **[no]device-role** {**host** | **monitor** | **router** | **switch**}
4. **[no]hop-limit** {**maximum** | **minimum**} *value*
5. **[no]managed-config-flag** {**off** | **on**}
6. **[no]match** {**ipv6 access-list** *list* | **ra prefix-list** *list*}
7. **[no]other-config-flag** {**on** | **off**}
8. **[no]router-preference maximum** {**high** | **medium** | **low**}
9. **[no]trusted-port**
10. **default** {**device-role** | **hop-limit** {**maximum** | **minimum**} | **managed-config-flag** | **match** {**ipv6 access-list** | **ra prefix-list** } | **other-config-flag** | **router-preference maximum**| **trusted-port**}
11. **do show ipv6 nd rguard policy** *policy_name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example: SwitchController# configure terminal</p>	Enters the global configuration mode.
Step 2	<p>[no]ipv6 nd rguard policy <i>policy-name</i></p> <p>Example: SwitchController(config)# ipv6 nd rguard policy example_policy</p>	Specifies the RA Guard policy name and enters RA Guard Policy configuration mode.
Step 3	<p>[no]device-role {host monitor router switch}</p> <p>Example: SwitchController(config-nd-raguard)# device-role switch</p>	Specifies the role of the device attached to the port. The default is host .
Step 4	<p>[no]hop-limit {maximum minimum} <i>value</i></p> <p>Example: SwitchController(config-nd-raguard)# hop-limit maximum 33</p>	<p>(1–255) Range for Maximum and Minimum Hop Limit values.</p> <p>Enables filtering of Router Advertisement messages by the Hop Limit value. A rogue RA message may have a low Hop Limit value (equivalent to the IPv4 Time to Live) that when accepted by the host, prevents the host from generating traffic to destinations beyond the rogue RA message generator. An RA message with an unspecified Hop Limit value is blocked.</p> <p>If not configured, this filter is disabled. Configure minimum to block RA messages with Hop Limit values lower than the value you specify. Configure maximum to block RA messages with Hop Limit values greater than the value you specify.</p>
Step 5	<p>[no]managed-config-flag {off on}</p> <p>Example: SwitchController(config-nd-raguard)# managed-config-flag on</p>	<p>Enables filtering of Router Advertisement messages by the Managed Address Configuration, or "M" flag field. A rouge RA message with an M field of 1 can cause a host to use a rogue DHCPv6 server. If not configured, this filter is disabled.</p> <p>On—Accepts and forwards RA messages with an M value of 1, blocks those with 0.</p> <p>Off—Accepts and forwards RA messages with an M value of 0, blocks those with 1.</p>
Step 6	<p>[no]match {ipv6 access-list <i>list</i> ra prefix-list <i>list</i>}</p> <p>Example: SwitchController(config-nd-raguard)# match ipv6 access-list example_list</p>	Matches a specified prefix list or access list.

	Command or Action	Purpose
Step 7	<p><code>[no]other-config-flag {on off}</code></p> <p>Example: <pre>SwitchController(config-nd-raguard)# other-config-flag on</pre></p>	<p>Enables filtering of Router Advertisement messages by the Other Configuration, or "O" flag field. A rouge RA message with an O field of 1 can cause a host to use a rogue DHCPv6 server. If not configured, this filter is disabled.</p> <p>On—Accepts and forwards RA messages with an O value of 1, blocks those with 0.</p> <p>Off—Accepts and forwards RA messages with an O value of 0, blocks those with 1.</p>
Step 8	<p><code>[no]router-preference maximum {high medium low}</code></p> <p>Example: <pre>SwitchController(config-nd-raguard)# router-preference maximum high</pre></p>	<p>Enables filtering of Router Advertisement messages by the Router Preference flag. If not configured, this filter is disabled.</p> <ul style="list-style-type: none"> • high—Accepts RA messages with the Router Preference set to high, medium, or low. • medium—Blocks RA messages with the Router Preference set to high. • low—Blocks RA messages with the Router Preference set to medium and high.
Step 9	<p><code>[no]trusted-port</code></p> <p>Example: <pre>SwitchController(config-nd-raguard)# trusted-port</pre></p>	<p>When configured as a trusted port, all attached devices are trusted, and no further message verification is performed.</p>
Step 10	<p><code>default {device-role hop-limit {maximum minimum} managed-config-flag match {ipv6 access-list ra prefix-list } other-config-flag router-preference maximum trusted-port}</code></p> <p>Example: <pre>SwitchController(config-nd-raguard)# default hop-limit</pre></p>	<p>Restores a command to its default value.</p>
Step 11	<p><code>do show ipv6 nd raguard policy <i>policy_name</i></code></p> <p>Example: <pre>SwitchController(config-nd-raguard)# do show ipv6 nd raguard policy example_policy</pre></p>	<p>(Optional)—Displays the ND Guard Policy configuration without exiting the RA Guard policy configuration mode.</p>

How to Attach an IPv6 Router Advertisement Guard Policy to an Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Router Advertisement policy to an interface or to VLANs on the interface :

SUMMARY STEPS

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **ipv6 nd rguard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]]
4. **do show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface Interface_type <i>stack/module/port</i> Example: SwitchController(config)# interface gigabitethernet 1/1/4	Specifies an interface type and identifier; enters the interface configuration mode.
Step 3	ipv6 nd rguard [attach-policy <i>policy_name</i> [vlan { <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }] vlan [{ <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }]] Example: SwitchController(config-if)# ipv6 nd rguard attach-policy <i>example_policy</i> or SwitchController(config-if)# ipv6 nd rguard attach-policy <i>example_policy</i> vlan 222,223,224 or SwitchController(config-if)# ipv6 nd rguard vlan 222,223,224	Attaches the Neighbor Discovery Inspection policy to the interface or the specified VLANs on that interface. The default policy is attached if the attach-policy option is not used.
Step 4	do show running-config Example: SwitchController#(config-if) # do show running-config	Confirms that the policy is attached to the specified interface without exiting the configuration mode.

How to Attach an IPv6 Router Advertisement Guard Policy to a Layer 2 EtherChannel Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Router Advertisement Guard Policy on an EtherChannel interface or VLAN:

SUMMARY STEPS

1. **configure terminal**
2. **interface range** *Interface_name*
3. **ipv6 nd rguard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]]
4. **do show running-config interface** *portchannel_interface_name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface range <i>Interface_name</i> Example: SwitchController(config)# interface Po11	Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode. Tip Enter the do show interfaces summary command for quick reference to interface names and types.
Step 3	ipv6 nd rguard [attach-policy <i>policy_name</i> [vlan { <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }] vlan [{ <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }]] Example: SwitchController(config-if-range)# ipv6 nd rguard attach-policy example_policy or SwitchController(config-if-range)# ipv6 nd rguard attach-policy example_policy vlan 222,223,224 or SwitchController(config-if-range)# ipv6 nd rguard vlan 222, 223,224	Attaches the RA Guard policy to the interface or the specified VLANs on that interface. The default policy is attached if the attach-policy option is not used.

	Command or Action	Purpose
Step 4	do show running-config interface <i>portchannel_interface_name</i> Example: SwitchController#(config-if-range)# do show running-config int poll	Confirms that the policy is attached to the specified interface without exiting the configuration mode.

How to Attach an IPv6 Router Advertisement Guard Policy to VLANs Globally

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Router Advertisement policy to VLANs regardless of interface:

SUMMARY STEPS

1. **configure terminal**
2. **vlan configuration** *vlan_list*
3. **ipv6 dhcp guard** [**attach-policy** *policy_name*]
4. **do show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 2	vlan configuration <i>vlan_list</i> Example: SwitchController(config)# vlan configuration 335	Specifies the VLANs to which the IPv6 RA Guard policy will be attached ; enters the VLAN interface configuration mode.
Step 3	ipv6 dhcp guard [attach-policy <i>policy_name</i>] Example: SwitchController(config-vlan-config)# ipv6 nd raguard attach-policy example_policy	Attaches the IPv6 RA Guard policy to the specified VLANs across all switch and stack interfaces. The default policy is attached if the attach-policy option is not used.
Step 4	do show running-config Example: SwitchController#(config-if)# do show running-config	Confirms that the policy is attached to the specified VLANs without exiting the configuration mode.

How to Configure an IPv6 DHCP Guard Policy

Beginning in privileged EXEC mode, follow these steps to configure an IPv6 DHCP (DHCPv6) Guard policy:

SUMMARY STEPS

1. **configure terminal**
2. **[no]ipv6 dhcp guard policy *policy-name***
3. **[no]device-role {client | server}**
4. **[no] match server access-list *ipv6-access-list-name***
5. **[no] match reply prefix-list *ipv6-prefix-list-name***
6. **[no]preference{ max *limit* | min *limit* }**
7. **[no] trusted-port**
8. **default {device-role | trusted-port}**
9. **do show ipv6 dhcp guard policy *policy_name***

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	[no]ipv6 dhcp guard policy <i>policy-name</i> Example: SwitchController(config)# ipv6 dhcp guard policy example_policy	Specifies the DHCPv6 Guard policy name and enters DHCPv6 Guard Policy configuration mode.
Step 3	[no]device-role {client server} Example: SwitchController(config-dhcp-guard) # device-role server	(Optional) Filters out DHCPv6 replies and DHCPv6 advertisements on the port that are not from a device of the specified role. Default is client . <ul style="list-style-type: none"> • client—Default value, specifies that the attached device is a client. Server messages are dropped on this port. • server—Specifies that the attached device is a DHCPv6 server. Server messages are allowed on this port.
Step 4	[no] match server access-list <i>ipv6-access-list-name</i> Example: ;;Assume a preconfigured IPv6 Access List as follows: SwitchController(config)# ipv6 access-list my_acls SwitchController(config-ipv6-acl) # permit host FE80::A8BB:CCFF:FE01:F700 any	(Optional). Enables verification that the advertised DHCPv6 server or relay address is from an authorized server access list (The destination address in the access list is 'any'). If not configured, this check will be bypassed. An empty access list is treated as a permit all.

	Command or Action	Purpose
	<pre>;;configure DHCPv6 Guard to match approved access list. SwitchController(config-dhcp-guard)# match server access-list my_acls</pre>	
Step 5	<p>[no] match reply prefix-list <i>ipv6-prefix-list-name</i></p> <p>Example:</p> <pre>;;Assume a preconfigured IPv6 prefix list as follows: SwitchController(config)# ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128 ;; Configure DHCPv6 Guard to match prefix SwitchController(config-dhcp-guard)# match reply prefix-list my_prefix</pre>	(Optional) Enables verification of the advertised prefixes in DHCPv6 reply messages from the configured authorized prefix list. If not configured, this check will be bypassed. An empty prefix list is treated as a permit.
Step 6	<p>[no] preference { max limit min limit }</p> <p>Example:</p> <pre>SwitchController(config-dhcp-guard)# preference max 250 SwitchController(config-dhcp-guard)#preference min 150</pre>	<p>Configure max and min when device-role is server to filter DHCPv6 server advertisements by the server preference value. The defaults permit all advertisements.</p> <p>max limit—(0 to 255) (Optional) Enables verification that the advertised preference (in preference option) is less than the specified limit. Default is 255. If not specified, this check will be bypassed.</p> <p>min limit—(0 to 255) (Optional) Enables verification that the advertised preference (in preference option) is greater than the specified limit. Default is 0. If not specified, this check will be bypassed.</p>
Step 7	<p>[no] trusted-port</p> <p>Example:</p> <pre>SwitchController(config-dhcp-guard)# trusted-port</pre>	<p>(Optional) trusted-port—Sets the port to a trusted mode. No further policing takes place on the port.</p> <p>Note If you configure a trusted port then the device-role option is not available.</p>
Step 8	<p>default { device-role trusted-port }</p> <p>Example:</p> <pre>SwitchController(config-dhcp-guard)# default device-role</pre>	(Optional) default —Sets a command to its defaults.
Step 9	<p>do show ipv6 dhcp guard policy <i>policy_name</i></p> <p>Example:</p> <pre>SwitchController(config-dhcp-guard)# do show ipv6 dhcp guard policy example_policy</pre>	(Optional) Displays the configuration of the IPv6 DHCP guard policy without leaving the configuration submode. Omitting the <i>policy_name</i> variable displays all DHCPv6 policies.

Example of DHCPv6 Guard Configuration

```
enable
configure terminal
ipv6 access-list acl1
```

```

permit host FE80::A8BB:CCFF:FE01:F700 any
ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
ipv6 dhcp guard policy poll
device-role server
match server access-list acl1
match reply prefix-list abc
preference min 0
preference max 255
trusted-port
interface GigabitEthernet 0/2/0
switchport
ipv6 dhcp guard attach-policy poll vlan add 1
vlan 1
  ipv6 dhcp guard attach-policy poll
show ipv6 dhcp guard policy poll

```

How to Attach an IPv6 DHCP Guard Policy to an Interface or a VLAN on an Interface

Beginning in privileged EXEC mode, follow these steps to configure IPv6 Binding Table Content :

SUMMARY STEPS

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **ipv6 dhcp guard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]]
4. **do show running-config interface** Interface_type *stack/module/port*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters the global configuration mode.
Step 2	interface Interface_type <i>stack/module/port</i> Example: SwitchController(config)# interface gigabitethernet 1/1/4	Specifies an interface type and identifier; enters the interface configuration mode.
Step 3	ipv6 dhcp guard [attach-policy <i>policy_name</i> [vlan { <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }] vlan [{ <i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all }]] Example: SwitchController(config-if)# ipv6 dhcp guard attach-policy example_policy or	Attaches the DHCP Guard policy to the interface or the specified VLANs on that interface. The default policy is attached if the attach-policy option is not used.

	Command or Action	Purpose
	<pre>SwitchController(config-if)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224 or SwitchController(config-if)# ipv6 dhcp guard vlan 222, 223,224</pre>	
Step 4	<p>do show running-config interface <i>Interface_type stack/module/port</i></p> <p>Example: <pre>SwitchController#(config-if)# do show running-config gig 1/1/4</pre></p>	Confirms that the policy is attached to the specified interface without exiting the configuration mode.

How to Attach an IPv6 DHCP Guard Policy to a Layer 2 EtherChannel Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 DHCP Guard policy on an EtherChannel interface or VLAN:

SUMMARY STEPS

1. **configure terminal**
2. **interface range** *Interface_name*
3. **ipv6 dhcp guard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]]
4. **do show running-config interface** *portchannel_interface_name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example: <pre>SwitchController# configure terminal</pre></p>	Enters the global configuration mode.
Step 2	<p>interface range <i>Interface_name</i></p> <p>Example: <pre>SwitchController(config)# interface Po11</pre></p>	<p>Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode.</p> <p>Tip Enter the do show interfaces summary command for quick reference to interface names and types.</p>

	Command or Action	Purpose
Step 3	<pre>ipv6 dhcp guard [attach-policy <i>policy_name</i> [vlan {<i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all}] vlan [{<i>vlan_ids</i> add <i>vlan_ids</i> except <i>vlan_ids</i> none remove <i>vlan_ids</i> all}]]</pre> <p>Example:</p> <pre>SwitchController(config-if-range)# ipv6 dhcp guard attach-policy example_policy</pre> <p>or</p> <pre>SwitchController(config-if-range)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224</pre> <p>or</p> <pre>SwitchController(config-if-range)#ipv6 dhcp guard vlan 222, 223,224</pre>	Attaches the DHCP Guard policy to the interface or the specified VLANs on that interface. The default policy is attached if the attach-policy option is not used.
Step 4	<pre>do show running-config interface <i>portchannel_interface_name</i></pre> <p>Example:</p> <pre>SwitchController#(config-if-range)# do show running-config int poll</pre>	Confirms that the policy is attached to the specified interface without exiting the configuration mode.

How to Attach an IPv6 DHCP Guard Policy to VLANs Globally

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 DHCP Guard policy to VLANs across multiple interfaces:

SUMMARY STEPS

1. **configure terminal**
2. **vlan configuration** *vlan_list*
3. **ipv6 dhcp guard** [attach-policy *policy_name*]
4. **do show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>configure terminal</pre> <p>Example:</p> <pre>SwitchController# configure terminal</pre>	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	<p>vlan configuration <i>vlan_list</i></p> <p>Example: SwitchController(config)# vlan configuration 334</p>	Specifies the VLANs to which the IPv6 Snooping policy will be attached ; enters the VLAN interface configuration mode.
Step 3	<p>ipv6 dhcp guard [attach-policy <i>policy_name</i>]</p> <p>Example: SwitchController(config-vlan-config)#ipv6 dhcp guard attach-policy example_policy</p>	Attaches the IPv6 Neighbor Discovery policy to the specified VLANs across all switch and stack interfaces. The default policy is attached if the attach-policy option is not used. The default policy is, device-role client , no trusted-port.
Step 4	<p>do show running-config</p> <p>Example: SwitchController#(config-if)# do show running-config</p>	Confirms that the policy is attached to the specified VLANs without exiting the configuration mode.

Additional References

Related Documents

Related Topic	Document Title
Implementing IPv6 Addressing and Basic Connectivity	http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-0sy/ipv6-addrg-bsc-con.html
IPv6 network management and security topics	IPv6 Configuration Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/xe-3se/3850/ipv6-xe-3se-3850-library.html
IPv6 Command Reference	IPv6 Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/command/ipv6-xe-3se-3850-cr-book.html

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

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support



Managing Rogue Devices

- [Finding Feature Information, page 457](#)
- [Information About Rogue Devices, page 457](#)
- [How to Configure Rogue Detection, page 462](#)
- [Monitoring Rogue Detection, page 464](#)
- [Examples: Rogue Detection Configuration, page 464](#)
- [Additional References for Rogue Detection, page 465](#)
- [Feature History and Information For Performing Rogue Detection Configuration, page 466](#)

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. Even more alarming, wireless users frequently publish unsecured access point locations, increasing the odds of having enterprise security breached.

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 nonmonitor 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**.

- 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.
- 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.

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.



Note

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 00x..... 0040 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.

Steps of how RLDP works are listed here:

- 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 with a severity of critical.

**Note**

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.

**Note**

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.

How to Configure Rogue Detection

Configuring Rogue Detection (CLI)

SUMMARY STEPS

1. `configure terminal`
2. `wireless wps rogue detection min-rssi rss in dBm`
3. `wireless wps rogue detection min-transient-time time in seconds`
4. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>configure terminal</code></p> <p>Example: SwitchController# <code>configure terminal</code></p>	Enters global configuration mode.
Step 2	<p><code>wireless wps rogue detection min-rssi <i>rss</i> in dBm</code></p> <p>Example: SwitchController(config)# <code>wireless wps rogue detection min-rssi 100</code></p>	<p>Specify the minimum RSSI value that rogues should have for APs to detect and for rogue entry to be created in the controller.</p> <p>Valid range for the <code>rss</code> in dBm parameter is -128 dBm to -70 dBm, and the default value is -128 dBm.</p> <p>Note This feature is applicable to all the AP modes. There can be many rogues with very weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs should detect rogues.</p>
Step 3	<p><code>wireless wps rogue detection min-transient-time <i>time</i> in seconds</code></p> <p>Example: SwitchController(config)# <code>wireless wps rogue detection min-transient-time</code></p>	<p>Specify the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned.</p> <p>Valid range for the <code>time</code> in sec parameter is 120 seconds to 1800 seconds, and the default value is 0.</p> <p>Note This feature is applicable to APs that are in monitor mode only.</p> <p>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.</p> <p>This feature has the following advantages:</p> <ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 4	end Example: SwitchController(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring Rogue Detection (GUI)

- 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** Choose **Configuration > Security > Wireless Protection Policies > Rogue Policies**. The **Rogue Policies** page is displayed.
- 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 controller.

Table 41: Monitoring Rogue Detection Command

Command	Purpose
<code>show wireless wps rogue ap summary</code>	Displays a list of all rogue access points detected by the controller.
<code>show wireless wps rogue client detailed <i>client-mac</i></code>	Displays detailed information for a specific rogue client.

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 controller:

```
SwitchController# configure terminal
SwitchController(config)# wireless wps rogue detection min-rssi -100
SwitchController(config)# end
SwitchController# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

This example shows how to configure the classification interval:

```
SwitchController# configure terminal
SwitchController(config)# wireless wps rogue detection min-transient-time 500
SwitchController(config)# end
SwitchController# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

Additional References for Rogue Detection

Related Documents

Related Topic	Document Title
Security commands	<i>Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/support</p>

Feature History and Information For Performing Rogue Detection Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.
Cisco IOS XE 3E	Rogue validation against MSE.



CHAPTER 22

Classifying Rogue Access Points

- [Finding Feature Information, page 467](#)
- [Information About Classifying Rogue Access Points, page 467](#)
- [Restrictions for Classifying Rogue Access Points, page 470](#)
- [How to Classify Rogue Access Points, page 471](#)
- [Viewing and Classifying Rogue Devices \(GUI\) , page 475](#)
- [Examples: Classifying Rogue Access Points, page 477](#)
- [Additional References for Classifying Rogue Access Points, page 478](#)
- [Feature History and Information For Classifying Rogue Access Points, page 479](#)

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 enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, and unclassified) in the Alert state only.

**Note**

Rule-based rogue classification does not apply to ad hoc rogues and rogue clients.

**Note**

You can configure up to 64 rogue classification rules per controller.

When the controller receives a rogue report from one of its managed access points, it responds as follows:

- 1 The controller verifies that the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.
- 2 If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.
- 3 If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.
- 4 The controller applies the first rule based on priority. If the rogue access point matches the criteria specified by the rule, the controller classifies the rogue according to the classification type configured for the rule.
- 5 If the rogue access point does not match any of the configured rules, the controller classifies the rogue as Unclassified.
- 6 The controller repeats the previous steps for all rogue access points.
- 7 If RLDP determines that the rogue access point is on the network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can then manually contain the rogue (unless you have configured RLDP to automatically contain the rogue), which would change the rogue state to Contained. If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.
- 8 If desired, you can manually move the access point to a different classification type and rogue state.

Table 42: Classification Mapping

Rule-Based Classification Type	Rogue States
Friendly	<ul style="list-style-type: none"> • Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. An example is the access points in your lab network. • External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. An example is an access point that belongs to a neighboring coffee shop. • Alert—The unknown access point is moved to Alert if it is not in the neighbor list or in the user-configured friendly MAC list.

Rule-Based Classification Type	Rogue States
Malicious	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 previously, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules, or you can manually move the unknown access point to a different classification type and rogue state.

Table 43: Allowable Classification Type and Rogue State Transitions

From	To
Friendly (Internal, External, Alert)	Malicious (Alert)
Friendly (Internal, External, Alert)	Unclassified (Alert)
Friendly (Alert)	Friendly (Internal, External)
Malicious (Alert, Threat)	Friendly (Internal, External)
Malicious (Contained, Contained Pending)	Malicious (Alert)
Unclassified (Alert, Threat)	Friendly (Internal, External)

From	To
Unclassified (Contained, Contained Pending)	Unclassified (Alert)
Unclassified (Alert)	Malicious (Alert)

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

Restrictions for Classifying Rogue Access Points

There are some rogue rules. They are:

- 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 using rogue rules.
- There are traps that are sent for containment by rule and for 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.
- Once a rogue satisfies a higher priority rule and 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.

How to Classify Rogue Access Points

Configuring Rogue Classification Rules (CLI)

SUMMARY STEPS

1. `configure terminal`
2. `wireless wps rogue rule rule-name priority priority`
3. `classify {friendly | malicious}`
4. `condition {client-count | duration | encryption | infrastructure | rssi | ssid}`
5. `match {all | any}`
6. `default`
7. `exit`
8. `shutdown`
9. `end`
10. `configure terminal`
11. `wireless wps rogue rule shutdown`
12. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>configure terminal</code></p> <p>Example: SwitchController# <code>configure terminal</code></p>	Enters global configuration mode.
Step 2	<p><code>wireless wps rogue rule <i>rule-name</i> priority <i>priority</i></code></p> <p>Example: SwitchController(config)# <code>wireless wps rogue rule rule_3 priority 3</code> SwitchController(config-rule)#</p>	<p>Creates or enables a rule. While creating a rule, you must enter priority for the rule.</p> <p>Note After creating the rule, if you are editing the rule, you can change the priority only for the rogue rules that are disabled. You cannot change priority for the rogue rules that are enabled. While editing, changing the priority for a rogue rule is optional.</p>
Step 3	<p><code>classify {friendly malicious}</code></p> <p>Example: SwitchController(config)# <code>wireless wps rogue rule rule_3 priority 3</code> SwitchController(config-rule)# <code>classify friendly</code></p>	Classifies a rule.

	Command or Action	Purpose
Step 4	<p>condition {client-count duration encryption infrastructure rfssi ssid}</p> <p>Example: <pre>SwitchController(config)# wireless wps rogue rule rule_3 priority 3 SwitchController(config-rule)# condition client-count 5</pre></p>	<p>Specifies to add the following conditions to a rule that the rogue access point must meet.</p> <ul style="list-style-type: none"> • client-count—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point for the <i>condition_value parameter</i>. The valid range is 1 to 10 (inclusive), and the default value is 0. • duration—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period for the <i>condition_value parameter</i>. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds. • encryption—Requires that the advertised WLAN does not have encryption enabled. • infrastructure—Requires the SSID to be known to the controller. • rfssi—Requires that the rogue access point have a minimum RSSI value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value for the <i>condition_value parameter</i>. The valid range is -95 to -50 dBm (inclusive), and the default value is 0 dBm. • ssid—Requires that the rogue access point have a specific SSID. You should add SSIDs that are not managed by the controller. If you choose this option, enter the SSID for the <i>condition_value parameter</i>. The SSID is added to the user-configured SSID list.
Step 5	<p>match {all any}</p> <p>Example: <pre>SwitchController(config)# wireless wps rogue rule rule_3 priority 3 SwitchController(config-rule)# match all</pre></p>	<p>Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule.</p>
Step 6	<p>default</p> <p>Example: <pre>SwitchController(config)# wireless wps rogue rule rule_3 priority 3 SwitchController(config-rule)# default</pre></p>	<p>Specifies to set a command to its default.</p>

	Command or Action	Purpose
Step 7	exit Example: SwitchController(config)# wireless wps rogue rule rule_3 priority 3 SwitchController(config-rule)# exit SwitchController(config)#	Specifies to exit the sub-mode.
Step 8	shutdown Example: SwitchController(config)# wireless wps rogue rule rule_3 priority 3 SwitchController(config-rule)# shutdown	Specifies to disable a particular rogue rule. For example, the rule rule_3 is disabled.
Step 9	end Example: SwitchController(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.
Step 10	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 11	wireless wps rogue rule shutdown Example: SwitchController(config)# wireless wps rogue rule shutdown	Specifies to disable all the rogue rules.
Step 12	end Example: SwitchController(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring Rogue Classification Rules (GUI)

- Step 1** Choose **Security > Wireless Protection Policies > Rogue Policies > Rogue Rules** to open the Rogue Rules page. Any rules that have already been created are listed in priority order. The name, type, and status of each rule is provided.
- Note** If you ever want to delete a rule, hover your mouse cursor over the blue drop-down arrow for that rule and click **Remove**.
- Step 2** Create a new rule as follows:
- Click **Add Rule**. An Add Rule section appears at the top of the page.
 - 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.

Note 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)

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.

Note A rogue access point cannot be moved to another class if its current state is Contain.

Step 5 From the Update Status drop-down list, choose one of the following options to specify how the controller should respond to this rogue access point:

- **Internal**—The controller trusts this rogue access point. This option is available if the Class Type is set to Friendly.
- **External**—The controller acknowledges the presence of this rogue access point. This option is available if the Class Type is set to Friendly.
- **Contain**—The controller contains the offending device so that its signals no longer interfere with authorized clients. This option is available if the Class Type is set to Malicious or Unclassified.
- **Alert**—The controller forwards an immediate alert to the system administrator for further action. This option is available if the Class Type is set to Malicious or Unclassified.

The bottom of the page provides information on both the access points that detected this rogue access point and any clients that are associated to it. To see more details for any of the clients, click **Edit** to open the Rogue Client Detail page.

Step 6 Click **Apply**.

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 rule that can organize and display rogue access points as Friendly:

```
SwitchController# configure terminal
SwitchController(config)# wireless wps rogue rule ap1 priority 1
SwitchController(config-rule)# classify friendly
SwitchController(config-rule)# end
```

This example shows how to apply condition that the rogue access point must meet:

```
SwitchController# configure terminal
SwitchController(config)# wireless wps rogue rule ap1 priority 1
SwitchController(config-rule)# condition client-count 5
```

```
SwitchController(config-rule)# condition duration 1000
SwitchController(config-rule)# end
```

Additional References for Classifying Rogue Access Points

Related Documents

Related Topic	Document Title
Security commands	<i>Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History and Information For Classifying Rogue Access Points

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.



CHAPTER 23

Configuring wIPS

- [Finding Feature Information, page 481](#)
- [Information About wIPS, page 481](#)
- [How to Configure wIPS on an Access Point, page 488](#)
- [Monitoring wIPS Information, page 490](#)
- [Examples: wIPS Configuration, page 490](#)
- [Additional References for Configuring wIPS, page 490](#)
- [Feature History for Performing wIPS Configuration, page 491](#)

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) is an advanced approach to wireless threat detection and performance management. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention. With a fully infrastructure-integrated solution, you can continually monitor wireless traffic on both the wired and wireless networks and use that network intelligence to analyze attacks from many sources to more accurately pinpoint and proactively prevent attacks rather than waiting until damage or exposure has occurred.

The Cisco Adaptive wIPS is enabled by the Cisco 3300 Series Mobility Services Engine (MSE), which centralizes the processing of intelligence collected by the continuous monitoring of Cisco Aironet access

points. With Cisco Adaptive wIPS functionalities and Cisco Prime Infrastructure integration into the MSE, the wIPS service can configure, monitor, and report wIPS policies and alarms.



Note If your wIPS deployment consists of a controller, access point, and MSE, you must set all the three entities to the UTC time zone.

The Cisco Adaptive wIPS is not configured on the controller. Instead, the Prime Infrastructure forwards the profile configuration to the wIPS service, which forwards the profile to the controller. The profile is stored in flash memory on the controller and sent to access points when they join the controller. When an access point disassociates and joins another controller, it receives the wIPS profile from the new controller.

Local mode access points with a subset of wIPS capabilities is referred to as Enhanced Local Mode access point or ELM AP. You can configure an access point to work in wIPS mode if the access point is in any of the following modes:

- Monitor
- Local

The regular local mode access point is extended with a subset of Wireless Intrusion Prevention System (wIPS) capabilities. This feature enables you to deploy your access points to provide protection without needing a separate overlay network.

wIPS ELM has limited capability of detecting off-channel alarms. The access point periodically goes off-channel, and monitors the non-serving channels for a short duration, and triggers alarms if any attack is detected on the channel. But the off-channel alarm detection is best effort and it takes longer time to detect attacks and trigger alarms, which might cause the ELM AP intermittently detect an alarm and clear it because it is not visible. Access points in any of the above modes can periodically send alarms based on the policy profile to the wIPS service through the controller. The wIPS service stores and processes the alarms and generates SNMP traps. The Prime Infrastructure configures its IP address as a trap destination to receive SNMP traps from the MSE.

This table lists all the SNMP trap controls and their respective traps. When a trap control is enabled, all the traps of the trap control are also enabled.



Note The controller uses only SNMPv2 for SNMP trap transmission.

Table 44: SNMP Trap Controls and their respective Traps

Tab Name	Trap Control	Trap
General	Link (Port) Up/Down	linkUp, linkDown
	Spanning Tree	newRoot, topologyChange, stpInstanceNewRootTrap, stpInstanceTopologyChangeTrap
	Config Save	bsnDot11EssCreated, bsnDot11EssDeleted, bsnConfigSaved, ciscoLwappScheduledResetNotif, ciscoLwappClearResetNotif, ciscoLwappResetFailedNotif, ciscoLwappSysInvalidXmlConfig
AP	AP Register	bsnAPDisassociated, bsnAPAssociated
	Ap Interface Up/Down	bsnAPIfUp, bsnAPIfDown
Client Traps	802.11 Association	bsnDot11StationAssociate
	802.11 Disassociation	bsnDot11StationDisassociate
	802.11 Deauthentication	bsnDot11StationDeauthenticate
	802.11 Failed Authentication	bsnDot11StationAuthenticateFail
	802.11 Failed Association	bsnDot11StationAssociateFail
	Exclusion	bsnDot11StationBlacklisted
	NAC Alert	cldcClientWlanProfileName, cldcClientIPAddress, cldcApMacAddress, cldcClientQuarantineVLAN, cldcClientAccessVLAN

Tab Name	Trap Control	Trap
Security Traps	User Authentication	bsnTooManyUnsuccessLoginAttempts, cLWAGuestUserLoggedIn, cLWAGuestUserLoggedOut
	RADIUS Servers Not Responding	bsnRADIUSServerNotResponding, ciscoLwappAAARadiusReqTimedOut
	WEP Decrypt Error	bsnWepKeyDecryptError
	Rogue AP	bsnAdhocRogueAutoContained, bsnRogueApAutoContained, bsnTrustedApHasInvalidEncryption, bsnMaxRogueCountExceeded, bsnMaxRogueCountClear, bsnApMaxRogueCountExceeded, bsnApMaxRogueCountClear, bsnTrustedApHasInvalidRadioPolicy, bsnTrustedApHasInvalidSsid, bsnTrustedApIsMissing
	SNMP Authentication	agentSnmpAuthenticationTrapFlag
	Multiple Users	multipleUsersTrap
Auto RF Profile Traps	Load Profile	bsnAPLoadProfileFailed
	Noise Profile	bsnAPNoiseProfileFailed
	Interference Profile	bsnAPInterferenceProfileFailed
	Coverage Profile	bsnAPCoverageProfileFailed
Auto RF Update Traps	Channel Update	bsnAPCurrentChannelChanged
	Tx Power Update	bsnAPCurrentTxPowerChanged

Tab Name	Trap Control	Trap
Mesh Traps	Child Excluded Parent	ciscoLwappMeshChildExcludedParent
	Parent Change	ciscoLwappMeshParentChange
	Authfailure Mesh	ciscoLwappMeshAuthorizationFailure
	Child Moved	ciscoLwappMeshChildMoved
	Excessive Parent Change	ciscoLwappMeshExcessiveParentChange
	Excessive Children	ciscoLwappMeshExcessiveChildren
	Poor SNR	ciscoLwappMeshAbateSNR, ciscoLwappMeshOnsetSNR
	Console Login	ciscoLwappMeshConsoleLogin
	Excessive Association	ciscoLwappMeshExcessiveAssociation
	Default Bridge Group Name	ciscoLwappMeshDefaultBridgeGroupName

The following are the trap description 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 controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

- Link (Port) Up/Down—Link changes status from up or down.
- Link (Port) Up/Down—Link changes status from up or down.
- Multiple Users—Two users log on 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 sent when the controller configuration is modified.

- Cisco AP Traps

- AP Register—Notification sent when an access point associates or disassociates with the controller.
- AP Interface Up/Down—Notification sent when an access point interface (802.11X) status goes up or down.

- Client Related Traps

- 802.11 Association—Associate notification that is sent when the client sends an association frame.
- 802.11 Disassociation—Disassociate notification that is sent when the client sends a disassociation frame.
- 802.11 Deauthentication—Deauthenticate notification that is sent when the client sends a deauthentication frame.
- 802.11 Failed Authentication—Authenticate failure notification that is sent when the 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).
- 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, have associated with the controller.
- 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 complete Layer2 authentication to inform about the client's presence to the NAC appliance. `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 associates with the controller or roams. The 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 controller. The data statistics include transmitted and received bytes and packets, SSID, and session ID.



Note When you downgrade to Release 7.4 from a higher 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 is to inform that a client RADIUS Authentication failure has occurred.
- RADIUS Server No Response—This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.
- WEP Decrypt Error—Notification sent when the controller detects a WEP decrypting error.
- 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 controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

- Multiple Users—Two users log on with the same ID.
- 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 sent when a defined number of failed association to the controller 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, it informs the controller.
 - Parent Change—Notification is sent by the agent when a child mesh node changes its parent. The child mesh node remembers its previous parent and it informs the controller about the change of its 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 then child mesh node informs the controller.
- Excessive Children—Notification sent when the child count exceeds for a RAP and MAP.
- Poor SNR—Notification sent when 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 than the object defined by 'clMeshSNRThresholdAbate'.
- Console Login—Notification is sent by the agent when login on MAP console is successful or failure after three attempts.
- Default Bridge Group Name—Notification sent when MAP mesh node joins parent using 'default' bridge group name.



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 controller cannot be turned off.



Note In all of the above cases, the controller functions solely as a forwarding device.



Note To download the MIBs, click [here](#).

How to Configure wIPS on an Access Point

Configuring wIPS on an Access Point (CLI)

SUMMARY STEPS

1. `ap name name mode submode wips`
2. `end`
3. `show wireless wps wips summary`
4. `show wireless wps wips statistics`

DETAILED STEPS

	Command or Action	Purpose
Step 1	ap name <i>name</i> mode submode <i>wips</i> Example: SwitchController# ap name ap1 mode local wips	Configure an access point for local or monitor mode and then set the submode to wIPS.
Step 2	end Example: SwitchController(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.
Step 3	show wireless wps wips summary Example: SwitchController# show wireless wps wips summary	View the wIPS configuration on the access point.
Step 4	show wireless wps wips statistics Example: SwitchController# show wireless wps wips statistics	View the current state of wIPS configuration.

Configuring wIPS on an Access Point (GUI)

-
- 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 controller.
- 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 45: Monitoring wIPS Command

Command	Purpose
<code>show wireless wps wips summary</code>	Displays the wIPS configuration on the access point.
<code>show wireless wps wips statistics</code>	Displays the current state of wIPS configuration.

Examples: wIPS Configuration

This example shows how to configure wIPS on AP1:

```
SwitchController# ap name ap1 mode local submode wips
SwitchController# end
SwitchController# show wireless wps wips summary
```

Additional References for Configuring wIPS

Related Documents

Related Topic	Document Title
wIPS commands	<i>Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All 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

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History for Performing wIPS Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.



Configuring Wireless Guest Access

- [Finding Feature Information, page 493](#)
- [Prerequisites for Guest Access, page 493](#)
- [Restrictions for Guest Access, page 494](#)
- [Information about Wireless Guest Access, page 494](#)
- [Fast Secure Roaming, page 494](#)
- [How to Configure Guest Access, page 495](#)
- [Configuration Examples for Guest Access, page 511](#)
- [Additional References for Guest Access, page 517](#)
- [Feature History and Information for Guest Access, page 518](#)

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 Guest Access

Guest Controller functionality is supported only on Catalyst 5760.

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), 802.11r 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, 802.11r to achieve the full requirements of fast secure roaming. The PMK cache (802.11i, CCKM, and 802.11r) 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

SUMMARY STEPS

1. **configure terminal**
2. **user-name** *user-name*
3. **type lobby-admin**
4. **password 0** *password*
5. **end**
6. **show running-config** | section *user-name* (or) **show running-config** | section *configured lobby admin* *username*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController # configure terminal	Enters global configuration mode.
Step 2	user-name <i>user-name</i> Example: SwitchController (config)# user-name lobby	Creates a user account.
Step 3	type lobby-admin Example: SwitchController (config-user-name)# type lobby-admin	Specifies the account type as lobby admin.
Step 4	password 0 <i>password</i> Example: SwitchController (config-user-name)# password 0 lobby	Creates a password for the lobby administrator account.
Step 5	end	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Example: SwitchController (config-user-name)# end	
Step 6	show running-config section <i>user-name</i> (or) show running-config section <i>configured lobby admin username</i> Example: SwitchController # show running-config section lobby	Displays the configuration details.

Configuring Guest User Accounts

SUMMARY STEPS

1. **configure terminal**
2. **user-name *user-name***
3. **password *unencrypted/hidden-password password***
4. **type network-user description *description* guest-user lifetime year *0-1* month *0-11* day *0-30* hour *0-23* minute *0-59* second *0-59***
5. **end**
6. **show aaa local netuser all**
7. **show running-config | section *user-name***

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController # configure terminal	Enters global configuration mode.
Step 2	user-name <i>user-name</i> Example: SwitchController (config)# user-name guest	Creates a username for the lobby ambassador account.
Step 3	password <i>unencrypted/hidden-password password</i> Example: SwitchController (config-user-name)# password 0 guest	Specifies the password for the user.

	Command or Action	Purpose
Step 4	<p>type network-user description <i>description</i> guest-user lifetime year <i>0-1</i> month <i>0-11</i> day <i>0-30</i> hour <i>0-23</i> minute <i>0-59</i> second <i>0-59</i></p> <p>Example: SwitchController (config-user-name)# type network-user description guest guest-user lifetime year 1 month 10 day 3 hour 1 minute 5 second 30</p>	Specifies the type of user.
Step 5	<p>end</p> <p>Example: SwitchController (config-user-name)# end</p>	Returns to privileged EXEC mode.
Step 6	<p>show aaa local netuser all</p> <p>Example: SwitchController # show aaa local netuser all</p>	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.
Step 7	<p>show running-config section<i>user-name</i></p> <p>Example: SwitchController # show running-config section guest</p>	Displays the configuration details.

Configuring Mobility Agent (MA)

SUMMARY STEPS

1. **configure terminal**
2. **wireless mobility controller ip***mc-ipaddress* **public-ip** *mc-publicipaddress*
3. **wlan** *wlan-name wlan-id ssid*
4. **client vlan id***vlan-group name/vlan-id*
5. **no security wpa**
6. **mobility anchor** *ipaddress*
7. **aaa-override**
8. **no shutdown**
9. **end**
10. **show wireless mobility summary**
11. **show wlan name** *wlan-name/id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController # configure terminal	Enters global configuration mode.
Step 2	wireless mobility controller ipmc-ipaddress public-ip mc-publicipaddress Example: SwitchController (config) # wireless mobility controller ip27.0.0.1 public-ip 27.0.0.1	Configures the Mobility Controller to which the MA will be associated.
Step 3	wlan wlan-name wlan-id ssid Example: SwitchController (config) # wlan mywlan 34 mywlan-ssid	<ul style="list-style-type: none"> • For <i>wlan-name</i> enter, enter the profile name. The range is 1- 32 characters. • For <i>wlan-id</i>, enter the WLAN ID. The range is 1-512. • For <i>ssid</i>, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.
Step 4	client vlan idvlan-group name/vlan-id Example: SwitchController (config-wlan) # client vlan VLAN0136	Configures the VLAN id or group of the WLAN.
Step 5	no security wpa Example: SwitchController (config-wlan) # 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.
Step 6	mobility anchor ipaddress Example: SwitchController (config-wlan) # mobility anchor 9.3.32.2	Configures the Guest Controller as mobility anchor.
Step 7	aaa-override Example: SwitchController (config-wlan) # aaa-override	(Optional) Enables AAA override. AAA override is required for non open authentication in case AAA attributes are to be prioritized. It is required only in case guest user need to be deauthenticated after lifetime or have to give aaa-override attribute to the user.
Step 8	no shutdown Example: SwitchController (config-wlan) # no shutdown	Enables the WLAN.
Step 9	end	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Example: SwitchController (config) # end	
Step 10	show wireless mobility summary Example: SwitchController # show wireless mobility summary	Verifies the mobility controller IP address and mobility tunnel status.
Step 11	show wlan name <i>wlan-name/id</i> Example: SwitchController # show wlan name mywlan	Displays the configuration of mobility anchor.

Configuring Mobility Controller

Mobility Controller mode should be enabled using the **wireless mobility controller** command.

SUMMARY STEPS

1. **configure terminal**
2. **wireless mobility group member ip** *ip-address* **public-ip** *ip-address* **group** *group-name*
3. **wireless mobility controller peer-group** *peer-group-name*
4. **wireless mobility controller peer-group** *peer-group-name* **member ip** *ipaddress* **public-ip** *ipaddress*
5. **end**
6. **show wireless mobility summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController # configure terminal	Enters global configuration mode.
Step 2	wireless mobility group member ip <i>ip-address</i> public-ip <i>ip-address</i> group <i>group-name</i> Example: SwitchController (config) # wireless mobility group member ip 27.0.0.1 public-ip 23.0.0.1 group test	Adds all peers within the MC group. The <i>ip-address</i> should be the guest controller's IP address.
Step 3	wireless mobility controller peer-group <i>peer-group-name</i>	Creates the switch peer group.

	Command or Action	Purpose
	Example: SwitchController (config) # wireless mobility controller peer-group pg	
Step 4	wireless mobility controller peer-group <i>peer-group-name</i> member ip <i>ipaddress</i> public-ip <i>ipaddress</i> Example: SwitchController (config) # wireless mobility controller peer-group pg member ip 9.7.136.10 public-ip 9.7.136.10	Adds the MA to the switch peer group.
Step 5	end Example: SwitchController (config) # end	Returns to privileged EXEC mode.
Step 6	show wireless mobility summary Example: SwitchController # show wireless mobility summary	Displays the configuration details.

Obtaining a Web Authentication Certificate

SUMMARY STEPS

1. **configure terminal**
2. **crypto pki import *trustpoint name* pkcs12 tftp: *passphrase***
3. **end**
4. **show crypto pki *trustpoints cert***

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController # configure terminal	Enters global configuration mode.
Step 2	crypto pki import <i>trustpoint name</i> pkcs12 tftp: <i>passphrase</i> Example: SwitchController (config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapsrvr-cert.p12 cisco	Imports certificate.

	Command or Action	Purpose
Step 3	end Example: SwitchController (config)# end	Returns to privileged EXEC mode.
Step 4	show crypto pki trustpoints cert Example: SwitchController # show crypto pki trustpoints cert	Displays the configuration details.

Displaying a Web Authentication Certificate

SUMMARY STEPS

1. **show crypto ca certificate verb**

DETAILED STEPS

	Command or Action	Purpose
Step 1	show crypto ca certificate verb Example: SwitchController # show crypto ca certificate verb	Displays the current web authentication certificate details.

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.

SUMMARY STEPS

1. **configure terminal**
2. **parameter-map type webauth** *parameter-map name*
3. **wlan** *wlan-name*
4. **shutdown**
5. **security web-auth**
6. **security web-auth authentication-list** *authentication list name*
7. **security web-auth parameter-map** *parameter-map name*
8. **no shutdown**
9. **end**
10. **show running-config** | section *wlan-name*
11. **show running-config** | section **parameter-map type webauth** *parameter-map*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController # configure terminal	Enters global configuration mode.
Step 2	parameter-map type webauth <i>parameter-map name</i> Example: SwitchController (config) # parameter-map type webauth test	Configures the web-auth parameter-map.
Step 3	wlan <i>wlan-name</i> Example: SwitchController (config) # wlan wlan10	For the wlan-name, enter the profile name. The range is 1- 32 characters.
Step 4	shutdown Example: SwitchController (config) # shutdown	Disables WLAN.
Step 5	security web-auth Example: Controller (config-wlan) # security web-auth	Enables web-auth on WLAN.
Step 6	security web-auth authentication-list <i>authentication list name</i> Example: Controller (config-wlan) # security web-auth authentication-list test	Allows you to map the authentication list name with the web-auth WLAN.

	Command or Action	Purpose
Step 7	security web-auth parameter-map <i>parameter-map name</i> Example: SwitchController (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: SwitchController (config) # no shutdown	Enables the WLAN.
Step 9	end Example: SwitchController (config) # end	Returns to privileged EXEC mode.
Step 10	show running-config section <i>wlan-name</i> Example: SwitchController# show running-config section mywlan	Displays the configuration details.
Step 11	show running-config section parameter-map type webauth <i>parameter-map</i> Example: SwitchController# show running-config section parameter-map type webauth test	Displays the configuration details.

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.

SUMMARY STEPS

1. **configure terminal**
2. **parameter-map type webauth global**
3. **virtual-ip {ipv4 | ipv6} ip-address**
4. **parameter-map type webauth** *parameter-map name*
5. **type {authbypass | consent | webauth | webconsent}**
6. **redirect [for-login|on-success|on-failure] URL**
7. **redirect portal {ipv4 | ipv6} ip-address**
8. **end**
9. **show running-config | section parameter-map**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController # configure terminal	Enters global configuration mode.
Step 2	parameter-map type webauth global Example: SwitchController (config) # parameter-map type webauth global	Configures a global webauth type parameter.
Step 3	virtual-ip {ipv4 ipv6} ip-address Example: SwitchController (config-params-parameter-map) # virtual-ip ipv4 1.1.1.1	Configures the virtual IP address.
Step 4	parameter-map type webauth parameter-map name Example: SwitchController (config-params-parameter-map) # parameter-map type webauth test	Configures the webauth type parameter.
Step 5	type {authbypass consent webauth webconsent} Example: SwitchController (config-params-parameter-map) # type webauth	Configures webauth subtypes such as consent, passthru, webauth, or webconsent.
Step 6	redirect [for-login on-success on-failure] URL Example: SwitchController (config-params-parameter-map) # redirect for-login http://9.1.0.100/login.html	Configures the redirect URL for the log in page, success page, and failure page.
Step 7	redirect portal {ipv4 ipv6} ip-address Example: SwitchController (config-params-parameter-map) # redirect portal ipv4 23.0.0.1	Configures the external portal IPv4 address.
Step 8	end Example: SwitchController (config-params-parameter-map) # end	Returns to privileged EXEC mode.
Step 9	show running-config section parameter-map Example: SwitchController # show running-config section parameter-map	Displays the configuration details.

Assigning Login, Login Failure, and Logout Pages per WLAN

SUMMARY STEPS

1. **configure terminal**
2. **parameter-map type webauth** *parameter-map-name*
3. **custom-page login device** *html-filename*
4. **custom-page login expired** *html-filename*
5. **custom-page failure device** *html-filename*
6. **custom-page success device** *html-filename*
7. **end**
8. **show running-config** | section **parameter-map type webauth** *parameter-map*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController # configure terminal	Enters global configuration mode.
Step 2	parameter-map type webauth <i>parameter-map-name</i> Example: SwitchController (config) # parameter-map type webauth test	Configures the webauth type parameter.
Step 3	custom-page login device <i>html-filename</i> Example: SwitchController (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 <i>html-filename</i> Example: SwitchController (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 <i>html-filename</i> Example: SwitchController (config-params-parameter-map)# custom-page failure device device flash:loginfail.html	Allows you to specify the filename for web authentication customized login failure page.
Step 6	custom-page success device <i>html-filename</i> Example: SwitchController (config-params-parameter-map)# custom-page success device device flash:loginsuccess.html	Allows you to specify the filename for web authentication customized login success page.

	Command or Action	Purpose
Step 7	end Example: SwitchController (config-params-parameter-map) # end	Returns to privileged EXEC mode.
Step 8	show running-config section parameter-map type webauth parameter-map Example: SwitchController (config) # show running-config section parameter-map type webauth test	Displays the configuration details.

Configuring AAA-Override

SUMMARY STEPS

1. **configure terminal**
2. **wlan *wlan-name***
3. **aaa-override**
4. **end**
5. **show running-config | section *wlan-name***

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController # configure terminal	Enters global configuration mode.
Step 2	wlan <i>wlan-name</i> Example: SwitchController (config) # wlan ramban	For <i>wlan-name</i> , enter the profile name. The range is 1- 32 characters.
Step 3	aaa-override Example: SwitchController (config-wlan) # aaa-override	Enables AAA override on the WLAN.
Step 4	end Example: SwitchController (config-wlan) # end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	show running-config section <i>wlan-name</i> Example: SwitchController # show running-config section ramban	Displays the configuration details.

Configuring Client Load Balancing

SUMMARY STEPS

1. **configure terminal**
2. **wlan *wlan-name***
3. **shutdown**
4. **mobility anchor *ip-address1***
5. **mobility anchor *ip-address2***
6. **no shutdown wlan**
7. **end**
8. **show running-config | section *wlan-name***

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController # configure terminal	Enters global configuration mode.
Step 2	wlan <i>wlan-name</i> Example: SwitchController (config)# wlan ramban	For <i>wlan-name</i> , enter the profile name.
Step 3	shutdown Example: SwitchController (config-wlan)# shutdown	Disables WLAN.
Step 4	mobility anchor <i>ip-address1</i> Example: SwitchController (config-wlan) # mobility anchor 9.7.136.15	Configures a guest controller as mobility anchor.

	Command or Action	Purpose
Step 5	mobility anchor <i>ip-address2</i> Example: SwitchController (config-wlan) # mobility anchor 9.7.136.16	Configures a guest controller as mobility anchor.
Step 6	no shutdown wlan Example: SwitchController (config-wlan) # no shutdown wlan	Enables the WLAN.
Step 7	end Example: SwitchController (config-wlan) # end	Returns to privileged EXEC mode.
Step 8	show running-config section <i>wlan-name</i> Example: SwitchController # show running-config section ramban	Displays the configuration details.

Configuring Preauthentication ACL

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *wlan-name*
3. **shutdown**
4. **ip access-group web** *preauthrule*
5. **no shutdown**
6. **end**
7. **show wlan name** *wlan-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 2	wlan <i>wlan-name</i>	For <i>wlan-name</i> , enter the profile name.

	Command or Action	Purpose
	Example: SwitchController (config)# wlan ramban	
Step 3	shutdown Example: SwitchController (config-wlan)# shutdown	Disables the WLAN.
Step 4	ip access-group web preauthrule Example: SwitchController (config-wlan)# ip access-group web preauthrule	Configures ACL that has to be applied before authentication.
Step 5	no shutdown Example: SwitchController (config)# no shutdown	Enables the WLAN.
Step 6	end Example: SwitchController (config-wlan)# end	Returns to privileged EXEC mode.
Step 7	show wlan name wlan-name Example: SwitchController# show wlan name ramban	Displays the configuration details.

Configuring IOS ACL Definition

SUMMARY STEPS

1. **configure terminal**
2. **ip access-list extended** *access-list number*
3. **permit udp any eq port number any**
4. **end**
5. **show access-lists** *ACL number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.

	Command or Action	Purpose
	Example: SwitchController # configure terminal	
Step 2	ip access-list extended <i>access-list number</i> Example: SwitchController (config) # ip access-list extended 102	Configures extended IP access-list.
Step 3	permit udp any eq <i>port number any</i> Example: SwitchController (config-ext-nacl) # permit udp any eq 8080 any	Configures destination host.
Step 4	end Example: SwitchController (config-wlan) # end	Returns to privileged EXEC mode.
Step 5	show access-lists <i>ACL number</i> Example: SwitchController # show access-lists 102	Displays the configuration details.

Configuring Webpassthrough

SUMMARY STEPS

1. **configure terminal**
2. **parameter-map type webauth** *parameter-map name*
3. **type consent**
4. **end**
5. **show running-config | section parameter-map type webauth** *parameter-map*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController # configure terminal	Enters global configuration mode.
Step 2	parameter-map type webauth <i>parameter-map name</i>	Configures the webauth type parameter.

	Command or Action	Purpose
	Example: SwitchController (config) # parameter-map type webauth webparalocal	
Step 3	type consent Example: SwitchController (config-params-parameter-map) # type consent	Configures webauth type as consent.
Step 4	end Example: SwitchController (config-params-parameter-map) # end	Returns to privileged EXEC mode.
Step 5	show running-config section parameter-map type webauth <i>parameter-map</i> Example: SwitchController (config) # show running-config section parameter-map type webauth test	Displays the configuration details.

Configuration Examples for Guest Access

Example: Creating a Lobby Ambassador Account

This example shows how to configure a lobby ambassador account.

```
SwitchController# configure terminal
SwitchController(config)# user-name lobby
SwitchController(config)# type lobby-admin
SwitchController(config)# password 0 lobby
SwitchController(config)# end
SwitchController# 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.

```
SwitchController# configure terminal
SwitchController(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapservers-cert.p12
cisco
SwitchController(config)# end
SwitchController# show crypto pki trustpoints cert
Trustpoint cert:
```

Example: Displaying a Web Authentication Certificate

```

Subject Name:
e=rkannajr@cisco.com
cn=sthaliya-lnx
ou=WNBU
o=Cisco
l=SanJose
st=California
c=US
    Serial Number (hex): 00
Certificate configured.
SwitchController# 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
o=Cisco
l=SanJose
st=California
c=US
Subject:
Name: ldapserver
e=rkannajr@cisco.com
cn=ldapserver
ou=WNBU
o=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:rkannajrcisc#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
o=Cisco
l=SanJose
st=California
c=US
Subject:
e=rkannajr@cisco.com
cn=sthaliya-lnx
ou=WNBU
o=Cisco
l=SanJose
st=California
c=US
Validity Date:
start date: 07:27:56 UTC Jan 31 2012
end date: 07:27:56 UTC Jan 28 2022
Associated Trustpoints: cert ldap12 ldap
Storage: nvram:rkannajrcisc#0CA.cer

```

Example: Displaying a Web Authentication Certificate

This example shows how to display a web authentication certificate.

```

SwitchController# show crypto ca certificate verb
Certificate

```

```

Status: Available
Version: 3
Certificate Serial Number (hex): 2A9636AC00000000858B
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:
http://www.cisco.com/security/pki/crl/cmca.crl
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.

```

SwitchController# configure terminal
SwitchController(config)# user-name guest
SwitchController(config-user-name)# password 0 guest
SwitchController(config-user-name)# type network-user description guest guest-user lifetime
year 1 month 10 day 3 hour 1 minute 5 second 30
SwitchController(config-user-name)# end
SwitchController# show aaa local netuser all
User-Name          : guest
Type               : guest
Password           : guest
Is_passwd_encrypted : No
Description        : guest
Attribute-List     : Not-Configured
First-Login-Time   : Not-Logged-In
Num-Login          : 0
Lifetime           : 1 years 10 months 3 days 1 hours 5 mins 30 secs
Start-Time         : 20:47:37 chennai Dec 21 2012

```

Example: Configuring Mobility Controller

This example shows how to configure a mobility controller.

```

SwitchController# configure terminal
SwitchController(config)# wireless mobility group member ip 27.0.0.1 public-ip 23.0.0.1
group test
SwitchController(config)# wireless mobility controller peer-group pg

```

Example: Choosing the Default Web Authentication Login Page

```
SwitchController(config)# wireless mobility controller peer-group pg member ip 9.7.136.10
public-ip 9.7.136.10
SwitchController(config)# end
SwitchController# 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 Domain ID for 802.11r : 0xac34
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:

IP	Public IP	Group Name	Multicast IP	Link Status
9.9.9.2	-	default	0.0.0.0	UP : UP
12.12.11.11	12.13.12.12	rasagna-grp		DOWN : DOWN
27.0.0.1	23.0.0.1	test		DOWN : DOWN

```
Switch Peer Group Name : spg1
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
```

IP	Public IP	Link Status
9.7.136.10	9.7.136.10	DOWN : DOWN

Example: Choosing the Default Web Authentication Login Page

This example shows how to choose a default web authentication login page.

```
SwitchController# configure terminal
SwitchController(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
SwitchController(config)# wlan wlan50
SwitchController(config-wlan)# shutdown
SwitchController(config-wlan)# security web-auth authentication-list test
SwitchController(config-wlan)# security web-auth parameter-map test
SwitchController(config-wlan)# no shutdown
SwitchController(config-wlan)# end
SwitchController# 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
```

```
SwitchController# 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 External Web Server

This example shows how to choose a customized web authentication login page from an external web server.

```
SwitchController# configure terminal
SwitchController(config)# parameter-map type webauth global
SwitchController(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1
SwitchController(config-params-parameter-map)# parameter-map type webauth test
SwitchController(config-params-parameter-map)# type webauth
SwitchController(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
SwitchController(config-params-parameter-map)# redirect portal ipv4 23.0.0.1
SwitchController(config-params-parameter-map)# end
SwitchController# 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 23.0.0.1
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.

```
SwitchController# configure terminal
SwitchController(config)# parameter-map type webauth test
SwitchController(config-params-parameter-map)# custom-page login device
flash:loginsantosh.html
SwitchController(config-params-parameter-map)# custom-page login expired device
flash:loginexpire.html
SwitchController(config-params-parameter-map)# custom-page failure device flash:loginfail.html
SwitchController(config-params-parameter-map)# custom-page success device
flash:loginsuccess.html
SwitchController(config-params-parameter-map)# end
SwitchController# show running-config | section parameter-map type webauth test
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 23.0.0.1
custom-page login device flash:loginsantosh.html
custom-page success device flash:loginsuccess.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.

```
SwitchController# configure terminal
SwitchController(config)# wlan fff
SwitchController(config-wlan)# aaa-override
SwitchController(config-wlan)# end
```

```
SwitchController# 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.

```
SwitchController# configure terminal
SwitchController(config)# wlan fff
SwitchController(config-wlan)# shutdown
SwitchController(config-wlan)# mobility anchor 9.7.136.15
SwitchController(config-wlan)# mobility anchor 9.7.136.16
SwitchController(config-wlan)# no shutdown wlan
SwitchController(config-wlan)# end
SwitchController# show running-config | section fff
wlan fff 44 fff
aaa-override
shutdown
```

Example: Configuring Preauthentication ACL

This example shows how to configure preauthentication ACL.

```
SwitchController# configure terminal
SwitchController(config)# wlan fff
SwitchController(config-wlan)# shutdown
SwitchController(config-wlan)# ip access-group web preauthrule
SwitchController(config-wlan)# no shutdown
SwitchController(config-wlan)# end
SwitchController# show wlan name fff
```

Example: Configuring IOS ACL Definition

This example shows how to configure IOS ACL definition.

```
SwitchController# configure terminal
SwitchController(config)# ip access-list extended 102
SwitchController(config-ext-nacl)# permit udp any eq 8080 any
SwitchController(config-ext-nacl)# end
SwitchController# 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.

```
SwitchController# configure terminal
SwitchController(config)# parameter-map type webauth webparalocal
SwitchController(config-params-parameter-map)# type consent
SwitchController(config-params-parameter-map)# end
SwitchController# show running-config | section parameter-map type webauth test
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 23.0.0.1
```

Additional References for Guest Access

Related Documents

Related Topic	Document Title
Mobility CLI commands	<i>Mobility Command Reference, Cisco IOS XE 3SE (Cisco WLC 5700 Series)</i>
Mobility configuration	<i>Mobility Configuration Guide, Cisco IOS XE 3SE (Cisco WLC 5700 Series)</i>
Security CLI commands	<i>Security Command Reference, Cisco IOS Release 3SE (Cisco WLC 5700 Series)</i>
Configuring web-based authentication on the Catalyst 5700 Series Wireless Controller	<i>Security Configuration Guide, Cisco IOS Release 3SE (Cisco WLC 5700 Series)</i>
Wired guest access configuration and commands	<i>Identity Based Networking Services</i>

Standards and RFCs

Standard/RFC	Title
None	-

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/support</p>

Feature History and Information for Guest Access

Releases	Feature Information
Cisco IOS XE Release 3.2SE	This feature was introduced.



Configuring Intrusion Detection System

- [Finding Feature Information, page 519](#)
- [Information About Intrusion Detection System, page 519](#)
- [How to Configure Intrusion Detection System, page 520](#)
- [Monitoring Intrusion Detection System, page 521](#)

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 <TBD>

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 Intrusion Detection System

The Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/CIPS) instructs controllers to block certain clients from accessing the wireless network when attacks involving these clients are detected at Layer 3 through Layer 7. This system offers significant network protection by helping to detect, classify, and stop threats including worms, spyware/adware, network viruses, and application abuse. Two methods are available to detect potential attacks:

- IDS sensors
- IDS signatures

IDS sensors can be configured to detect various types of IP-level attacks in the network. When the sensors identify an attack, they can alert the controller to shun the offending client. When a new IDS sensor is added, the IDS sensor should be registered with the controller so that the controller can query the sensor to get the list of shunned clients.

When an IDS sensor detects a suspicious client, it alerts the controller to shun this client. The shun entry is distributed to all controllers within the same mobility group. If the client to be shunned is currently joined to a controller in this mobility group, the anchor controller adds this client to the dynamic exclusion list, and the foreign controller removes the client. The next time that the client tries to connect to a controller, the anchor controller rejects the handoff and informs the foreign controller that the client is being excluded.

How to Configure Intrusion Detection System

Configuring IDS Sensors

SUMMARY STEPS

1. **configure terminal**
2. **wireless wps cids-sensor *index* [ip-address *ip-addr* username *username* password *password_type* password]**
3. **wireless wps cids-sensor *index***
4. **[default exit fingerprint interval no port shutdown]**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchController# configure terminal	Enters global configuration mode.
Step 2	wireless wps cids-sensor <i>index</i> [ip-address <i>ip-addr</i> username <i>username</i> password <i>password_type</i> password] Example: SwitchController(config)# wireless wps cids-sensor 2 231.1.1.1 admin pwd123	Configures the IDS sensors that holds and internal index number. The index parameter determines the sequence in which the controller consults the IDS sensors. The controller supports up to five IDS sensors. <ul style="list-style-type: none"> • ip-address– [optional] Provide the IP address for the IDS. • username– [optional] Configures the username for the IDS. • password– [optional] Configures the password for the respective username.
Step 3	wireless wps cids-sensor <i>index</i> Example: SwitchController(config)# wireless wps cids-sensor 1	Enters the IDS configuration submode.
Step 4	[default exit fingerprint interval no port shutdown]	Configures various IDS parameters. <ul style="list-style-type: none"> • default– [optional] Sets a command to its default.

	Command or Action	Purpose
	Example: <pre>SwitchController(config-cids-index)# default</pre>	<ul style="list-style-type: none"> • exit- [optional] Exits the submode. • fingerprint- [optional] Configures the sensor's TLS fingerprint. • interval- [optional] Configures the sensor's query interval. The range is between 10-3600 seconds. • no- [optional] Negates a command or set its defaults. • port- [optional] Configures the sensor's port number. • shutdown- [optional] Shuts down the intrusion detection sensor.
Step 5	end Example: <pre>SwitchController(config)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Monitoring Intrusion Detection System

Table 46: Commands for Monitoring Wireless Multicast

Commands	Description
show wireless wps cids-sensor <i>index</i>	Displays the IDS configuration of the IDS sensor with the mentioned index value.
show wireless wps cids-sensor summary	Displays the list of all the configured IDS with their respective values like index, ip-address, port number, interval value, status and last query.
show wireless wps shun-list	Displays the list of the IDS shun list.



INDEX

802.1x [237](#)

A

- access control entries [156](#)
 - See ACEs [156](#)
- access groups [169](#)
 - Layer 3 [169](#)
- access groups, applying IPv4 ACLs to interfaces [182](#)
- access lists [161](#)
 - See ACLs [161](#)
- accounting [45, 56, 84](#)
 - with RADIUS [84](#)
 - with TACACS+ [45, 56](#)
- accounting, defined [45](#)
- ACEs [156](#)
 - Ethernet [156](#)
 - IP [156](#)
- ACLs [156, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 178, 180, 182, 187, 192, 194, 204, 205, 206](#)
 - applying [178, 182, 204, 205, 206](#)
 - on routed packets [205](#)
 - on bridged packets [204](#)
 - on multicast packets [206](#)
 - on switched packets [204](#)
 - time ranges to [178](#)
 - to an interface [182](#)
 - comments in [194](#)
 - compiling [194](#)
 - defined [161](#)
 - examples of [194](#)
 - extended IPv4 [161, 171](#)
 - creating [171](#)
 - matching criteria [161](#)
 - interface [169](#)
 - IP [161, 163, 169, 178](#)
 - implicit deny [178](#)
 - implicit masks [163](#)
 - matching criteria [161](#)
 - undefined [169](#)
- ACLs (*continued*)
 - IPv4 [161, 162, 169, 180, 182](#)
 - applying to interfaces [182](#)
 - creating [161](#)
 - interfaces [169](#)
 - matching criteria [161](#)
 - numbers [162](#)
 - terminal lines, setting on [180](#)
 - unsupported features [161](#)
 - Layer 4 information in [167](#)
 - logging messages [164](#)
 - matching [169](#)
 - monitoring [192](#)
 - port [156](#)
 - precedence of [156](#)
 - router [156](#)
 - router ACLs and VLAN map configuration guidelines [167](#)
 - standard IPv4 [161, 170](#)
 - creating [170](#)
 - matching criteria [161](#)
 - support in hardware [165](#)
 - time ranges to [168](#)
 - types supported [156](#)
 - unsupported features [161](#)
 - IPv4 [161](#)
 - using router ACLs with VLAN maps [167](#)
 - VLAN maps [166, 187](#)
 - configuration guidelines [166](#)
 - configuring [187](#)
- adding [238, 240](#)
- and SSH [134](#)
- attributes [87, 89](#)
 - vendor-proprietary [89](#)
 - vendor-specific [87](#)
- attributes, RADIUS [87, 89, 95](#)
 - vendor-proprietary [89, 95](#)
 - vendor-specific [87](#)
- authenticating to [103, 104](#)
 - boundary switch [103](#)
 - KDC [103](#)
 - network services [104](#)

authentication [45, 49, 51, 74, 77, 107](#)
 local mode with AAA [107](#)
 RADIUS [74, 77](#)
 key [74](#)
 login [77](#)
 TACACS+ [45, 49, 51](#)
 defined [45](#)
 key [49](#)
 login [51](#)
 authentication key [49](#)
 authentication, defined [45](#)
 authorization [45, 54, 82](#)
 with RADIUS [82](#)
 with TACACS+ [45, 54](#)
 authorization, defined [45](#)
 automatic [235](#)

B

Berkeley r-tools replacement [134](#)
 binding configuration [235](#)
 automatic [235](#)
 manual [235](#)
 binding database [214](#)
 address, DHCP server [214](#)
 See DHCP, Cisco IOS server database [214](#)
 binding table [235](#)
 bindings [214, 235](#)
 address, Cisco IOS DHCP server [214](#)
 IP source guard [235](#)
 boundary switch [103](#)
 bridged packets, ACLs on [204](#)

C

CA trustpoint [142, 144](#)
 configuring [144](#)
 defined [142](#)
 Change Rules Priority parameter [475](#)
 changing the default for lines [38](#)
 CipherSuites [143](#)
 Cisco 3300 Series Mobility Services Engine (MSE), using with wIPS [481](#)
 Cisco IOS DHCP server [214](#)
 See DHCP, Cisco IOS DHCP server [214](#)
 CoA Request Commands [68](#)
 commands, setting privilege levels [36](#)
 communication, global [74, 86](#)
 communication, per-server [74](#)
 configuration examples [100](#)

Configuration Examples for Setting Passwords and Privilege Levels command [40](#)
 configuration files [30](#)
 password recovery disable considerations [30](#)
 configuration guidelines [144, 237](#)
 configuring [49, 51, 54, 56, 74, 77, 82, 84, 86, 104, 134, 144, 146, 149](#)
 accounting [56, 84](#)
 authentication [77](#)
 authentication key [49](#)
 authorization [54, 82](#)
 communication, global [74, 86](#)
 communication, per-server [74](#)
 login authentication [51](#)
 multiple UDP ports [74](#)
 configuring a secure HTTP client [149](#)
 configuring a secure HTTP server [146](#)
 Configuring Local Web Authentication Using RADIUS Server (GUI) [117](#)
 Configuring the Switch for Vendor-Proprietary RADIUS Server Communication [95](#)
 Example command [95](#)
 Configuring the Switch to Use Vendor-Specific RADIUS Attributes [95](#)
 Examples command [95](#)
 credentials [100](#)
 customizable web pages, web-based authentication [366](#)

D

default configuration [24, 49, 71, 144](#)
 password and privilege level [24](#)
 RADIUS [71](#)
 SSL [144](#)
 TACACS+ [49](#)
 default web-based authentication configuration [370](#)
 802.1X [370](#)
 defined [45, 142](#)
 defining AAA server groups [79](#)
 described [100, 141, 235](#)
 Detect and Report Adhoc Networks parameter [463](#)
 DHCP [209, 218](#)
 enabling [209, 218](#)
 relay agent [218](#)
 server [209](#)
 DHCP option 82 [211, 219, 227](#)
 displaying [227](#)
 forwarding address, specifying [219](#)
 helper address [219](#)
 overview [211](#)
 DHCP server port-based address allocation [228, 231](#)
 default configuration [228](#)
 enabling [231](#)

DHCP snooping [210, 211, 235](#)
 accepting untrusted packets form edge switch [210](#)
 option 82 data insertion [211](#)
 trusted interface [210](#)
 untrusted messages [210](#)

DHCP snooping binding database [214, 215, 222, 229](#)
 adding bindings [229](#)
 binding file [215](#)
 format [215](#)
 location [215](#)
 configuration guidelines [222](#)
 configuring [229](#)
 described [214](#)
 enabling [229](#)

disabling recovery of [30](#)

displaying [150](#)

E

enable [26](#)

enable password [28](#)

enable secret [28](#)

enable secret password [28](#)

enabling [238, 240](#)

encrypting [28](#)

encryption for passwords [28](#)

encryption methods [133](#)

encryption, CipherSuite [143](#)

EtherChannels [237](#)

Examples for controlling switch access with RADIUS [94](#)

exiting [39](#)

Expiration Timeout for Rogue AP and Rogue Client Entries parameter [463](#)

F

filtering [183](#)
 non-IP traffic [183](#)

filters, IP [155](#)
 See ACLs, IP [filters [155](#)
 IP [155](#)
 zzz] [155](#)

G

Guest Users [118](#)

H

HTTP over SSL [141](#)
 see HTTPS [141](#)

HTTP secure server [141](#)

HTTPS [141, 142, 146](#)
 configuring [146](#)
 described [141](#)
 self-signed certificate [142](#)

I

ICMP [155, 165](#)
 unreachable messages [155](#)
 unreachables and ACLs [165](#)

Identifying the RADIUS Server Host [94](#)
 Examples command [94](#)

identifying the server [49, 74](#)

IP ACLs [164](#)
 named [164](#)

IP source guard [235, 237, 238, 240](#)
 802.1x [237](#)
 binding configuration [235](#)
 automatic [235](#)
 manual [235](#)
 binding table [235](#)
 configuration guidelines [237](#)
 described [235](#)
 DHCP snooping [235](#)
 enabling [238, 240](#)
 EtherChannels [237](#)
 port security [237](#)
 routed ports [237](#)
 static bindings [238, 240](#)
 adding [238, 240](#)
 static hosts [240](#)
 TCAM entries [237](#)
 trunk interfaces [237](#)
 VRF [237](#)

IPv4 ACLs [169, 170, 171, 175, 182](#)
 applying to interfaces [182](#)
 extended, creating [171](#)
 interfaces [169](#)
 named [175](#)
 standard, creating [170](#)

K

KDC [100, 103](#)
 described [100](#)

KDC (*continued*)

See also Kerberos[KDC 100
zzz] 100

Kerberos 100, 103, 104

authenticating to 103, 104

boundary switch 103

KDC 103

network services 104

configuration examples 100

configuring 104

credentials 100

described 100

KDC 100

operation 103

realm 100

server 100

switch as trusted third party 100

terms 100

TGT 100

tickets 100

key 49, 74

key distribution center 100

See KDC 100

L

limiting the services to the user 54, 82

local mode with AAA 107

logging into 39

logging messages, ACL 164

login 51, 77

login authentication 51, 77

with RADIUS 77

with TACACS+ 51

M

MAC extended access lists 155, 185

applying to Layer 2 interfaces 155, 185

manual 235

monitoring 150, 192, 193

access groups 192

IPv4 ACL configuration 192

VLAN 193

maps 193

filters 193

multicast packets 206

ACLs on 206

multiple UDP ports 74

N

network services 104

non-IP traffic filtering 183

O

operation 103

operation of 47, 64

overview 21, 26, 45, 63

P

Parameter Map for Local Web Authentication 122

password and privilege level 24

password recovery disable considerations 30

passwords 21, 24, 26, 28, 30, 32, 34

default configuration 24

disabling recovery of 30

encrypting 28

overview 21

setting 26, 28, 32, 34

enable 26

enable secret 28

Telnet 32

with usernames 34

persistent self-signed certificate 142

port ACLs 156, 157

defined 156

types of 157

port security 237

port-based authentication 362, 370, 371, 372, 376, 387

configuration guidelines 371

configuring 372, 376

RADIUS server 372

RADIUS server parameters on the switch 376

default configuration 370

device roles 362

displaying statistics 387

enabling 376

802.1X authentication 376

switch 362

as proxy 362

preventing unauthorized access 21

privilege levels 26, 36, 38, 39

changing the default for lines 38

exiting 39

logging into 39

overview 26

setting a command with 36

Protecting Enable and Enable Secret Passwords with Encryption [41](#)
 Example command [41](#)

R

RADIUS [63, 64, 71, 74, 77, 79, 82, 84, 86, 87, 89, 95](#)
 attributes [87, 89, 95](#)
 vendor-proprietary [89, 95](#)
 vendor-specific [87](#)
 configuring [74, 77, 82, 84, 86](#)
 accounting [84](#)
 authentication [77](#)
 authorization [82](#)
 communication, global [74, 86](#)
 communication, per-server [74](#)
 multiple UDP ports [74](#)
 default configuration [71](#)
 defining AAA server groups [79](#)
 identifying the server [74](#)
 key [74](#)
 limiting the services to the user [82](#)
 login [77](#)
 operation of [64](#)
 overview [63](#)
 suggested network environments [63](#)
 tracking services accessed by user [84](#)
RADIUS Change of Authorization [65](#)
 realm [100](#)
 Remote Authentication Dial-In User Service [63](#)
 See RADIUS [63](#)
 restricting access [21, 45, 63](#)
 overview [21](#)
 RADIUS [63](#)
 TACACS+ [45](#)
 RFC 5176 Compliance [66](#)
 RLDP. See Rogue Location Discovery Protocol (RLDP) [460](#)
 rogue access points [463](#)
 automatically containing [463](#)
 using the GUI [463](#)
 Rogue Detection parameter [463](#)
 Rogue Location Discovery Protocol parameter [463](#)
 Rogue Policies page [463](#)
 rogue states [469](#)
 routed packets, ACLs on [205](#)
 routed ports [237](#)
 router ACLs [156, 158](#)
 defined [156](#)
 types of [158](#)

S

SCP [134](#)
 and SSH [134](#)
 configuring [134](#)
 Secure Copy Protocol
 secure HTTP client [149, 150](#)
 configuring [149](#)
 displaying [150](#)
 secure HTTP server [146, 150](#)
 configuring [146](#)
 displaying [150](#)
 Secure Shell [133](#)
 See also Kerberos[KDC [100](#)
 zzz] [100](#)
 see HTTPS [141](#)
 See KDC [100](#)
 See RADIUS [63](#)
 See SCP [134](#)
 See TACACS+ [45](#)
 self-signed certificate [142](#)
 server [100](#)
 setting [26, 28, 32, 34](#)
 enable [26](#)
 enable secret [28](#)
 Telnet [32](#)
 with usernames [34](#)
 setting a command with [36](#)
 setting a password [32](#)
 Setting a Telnet Password for a Terminal Line [41](#)
 Example command [41](#)
 Setting or Changing a Static Enable Password [40](#)
 Example command [40](#)
 Setting the Privilege Level for a Command [41](#)
 Example command [41](#)
 show access-lists hw-summary command [165](#)
SSH [132, 133](#)
 encryption methods [133](#)
 user authentication methods, supported [133](#)
SSH server [136](#)
SSL [144, 146, 149, 150](#)
 configuration guidelines [144](#)
 configuring a secure HTTP client [149](#)
 configuring a secure HTTP server [146](#)
 monitoring [150](#)
 stack changes, effects on [161](#)
 ACL configuration [161](#)
 static bindings [238, 240](#)
 adding [238, 240](#)
 static hosts [240](#)
 statistics [387](#)
 802.1X [387](#)
 suggested network environments [63](#)

SVIs [158](#)
 and router ACLs [158](#)
 Switch Access [40](#)
 displaying [40](#)
 switch as trusted third party [100](#)
 switched packets, ACLs on [204](#)

T

TACACS+ [45, 47, 49, 51, 54, 56, 58](#)
 accounting, defined [45](#)
 authentication, defined [45](#)
 authorization, defined [45](#)
 configuring [49, 51, 54, 56](#)
 accounting [56](#)
 authentication key [49](#)
 authorization [54](#)
 login authentication [51](#)
 default configuration [49](#)
 defined [45](#)
 displaying [58](#)
 identifying the server [49](#)
 key [49](#)
 limiting the services to the user [54](#)
 login [51](#)
 operation of [47](#)
 overview [45](#)
 tracking services accessed by user [56](#)
 TCAM entries [237](#)
 Telnet [32](#)
 setting a password [32](#)
 temporary self-signed certificate [142](#)
 Terminal Access Controller Access Control System Plus [45](#)
 See TACACS+ [45](#)
 terminal lines, setting a password [32](#)
 terms [100](#)
 TGT [100](#)
 tickets [100](#)
 time ranges in ACLs [168, 178](#)
 time-range command [168](#)
 tracking services accessed by user [56, 84](#)
 traffic [159, 160](#)
 fragmented [159, 160](#)
 trunk interfaces [237](#)

trustpoints, CA [142](#)

U

user authentication methods, supported [133](#)
 username-based authentication [34](#)

V

Validate Rogue Clients Against AAA parameter [463](#)
 vendor-proprietary [89](#)
 vendor-specific [87](#)
 VLAN map entries, order of [166](#)
 VLAN maps [166, 187, 188, 189, 190, 191, 193, 202, 203](#)
 applying [191](#)
 common uses for [202](#)
 configuration guidelines [166](#)
 configuring [187](#)
 creating [189](#)
 denying access to a server example [203](#)
 denying and permitting packets [188, 190](#)
 displaying [193](#)
 VRF [237](#)

W

web-based authentication [361, 366](#)
 customizeable web pages [366](#)
 description [361](#)
 web-based authentication, interactions with other features [369](#)
 wireless intrusion prevention system (wIPS) [481](#)
 described [481](#)
 with RADIUS [77, 82, 84](#)
 with TACACS+ [45, 51, 54, 56](#)
 with usernames [34](#)

Z

zzz] [100](#)