CONTENTS

CHAPTER 1

Preventing Unauthorized Access 1
Finding Feature Information 1
Preventing Unauthorized Access 1
Feature Information for Preventing Unauthorized Access 2

CHAPTER 2

Controlling Switch Access with Passwords and Privilege Levels 3
Restrictions for Controlling Switch Access with Passwords and Privilege Levels 3
Information About Passwords and Privilege Levels 4
Default Password and Privilege Level Configuration 4
Additional Password Security 4
Password Recovery 4
Terminal Line Telnet Configuration 5
Username and Password Pairs 5
Privilege Levels 5
How to Control Switch Access with Passwords and Privilege Levels 6
Setting or Changing a Static Enable Password 6
Protecting Enable and Enable Secret Passwords with Encryption 7
Disabling Password Recovery 9
Setting a Telnet Password for a Terminal Line 10
Configuring Username and Password Pairs 11
Setting the Privilege Level for a Command 13
Changing the Default Privilege Level for Lines 14
Logging into and Exiting a Privilege Level 15
Monitoring Switch Access 15
Configuration Examples for Setting Passwords and Privilege Levels 16
Example: Setting or Changing a Static Enable Password 16
CHAPTER 3

Configuring Authentication 19

Prerequisites for Configuring Authentication 19
Restrictions for Configuring Authentication 19
Information About Configuring Authentication 20
Named Method Lists for Authentication 20
  Method Lists and Server Groups 20
  Method List Examples 21
About RADIUS Change of Authorization 22
  CoA Requests 23
  CoA Request Response Code 24
  CoA Request Commands 25
Domain Stripping 27

How to Configure AAA Authentication Methods 27
Configuring Login Authentication Using AAA 27
  Login Authentication Using Enable Password 29
  Login Authentication Using Kerberos 29
  Login Authentication Using Line Password 30
  Login Authentication Using Local Password 30
  Login Authentication Using Group RADIUS 30
  Configuring RADIUS Attribute 8 in Access Requests 30
  Login Authentication Using Group TACACS 30
  Login Authentication Using group-group-name 31
Configuring PPP Authentication Using AAA 31
  PPP Authentication Using Kerberos 33
  PPP Authentication Using Local Password 33
  PPP Authentication Using Group RADIUS 33
  Configuring RADIUS Attribute 44 in Access Requests 34
  PPP Authentication Using Group TACACS 34
Configuring Domain Stripping at the Server Group Level 53
Non-AAA Authentication Methods 53
    Configuring Line Password Protection 53
    Establishing Username Authentication 54
    Enabling CHAP or PAP Authentication 55
Using MS-CHAP 59
    Defining PPP Authentication using MS-CHAP 60
Authentication Examples 61
    Example: RADIUS Authentication 61
    Example: TACACS Authentication 62
    Example: Kerberos Authentication 63
    Example: AAA Scalability 63
    Example: Configuring Login and Failed-Login Banners for AAA Authentication 64
    Example: AAA Packet of Disconnect Server Key 65
    Example: Double Authentication 65
    Example: Automated Double Authentication 70
Additional References for Configuring Authentication 72
Feature Information for Configuring Authentication 73

CHAPTER 4
Configuring Authorization 75
AAA Authorization Prerequisites 75
Information About Configuring Authorization 76
    Named Method Lists for Authorization 76
    AAA Authorization Methods 76
    Authorization Methods 77
    Method Lists and Server Groups 78
    AAA Authorization Types 78
    Authorization Types 78
    Authorization Attribute-Value Pairs 79
How to Configure Authorization 79
    Configuring AAA Authorization Using Named Method Lists 79
    Disabling Authorization for Global Configuration Commands 80
    Configuring Authorization for Reverse Telnet 80
Authorization Configuration Examples 81
chapter 5

configuring accounting 87

prerequisites for configuring accounting 87
restrictions for configuring accounting 87

topic 2.1 88

information about configuring accounting 88

named method lists for accounting 88

method lists and server groups 89

aaa accounting methods 89

aaa accounting types 91

network accounting 91

exec accounting 93

command accounting 95

connection accounting 95

system accounting 97

resource accounting 98

aaa accounting enhancements 100

aaa broadcast accounting 100

aaa session mib 100

accounting attribute-value pairs 101

how to configure aaa accounting 101

configuring aaa accounting using named method lists 101

suppressing generation of accounting records for null username sessions 103

generating interim accounting records 103

configuring an alternate method to enable periodic accounting records 103

generating interim service accounting records 104

generating accounting records for a failed login or session 105

specifying accounting network-stop records before exec-stop records 105

suppressing system accounting records over switchover 106
CHAPTER 6  Configuring Local Authentication and Authorization 115
How to Configure Local Authentication and Authorization 115
Configuring the Switch for Local Authentication and Authorization 115
Monitoring Local Authentication and Authorization 117
Additional References 117
Feature Information for Local Authentication and Authorization 118

CHAPTER 7  Configuring TACACS+ 119
Prerequisites for TACACS+ 119
Information About Controlling Switch Access with TACACS+ 120
TACACS+ and Switch Access 120
TACACS+ Overview 120
TACACS+ Operation 121
Method List 122
TACACS+ Configuration Options 123
TACACS+ Login Authentication 123
TACACS+ Authorization for Privileged EXEC Access and Network Services 123
TACACS+ Accounting 123
Default TACACS+ Configuration 123
How to Configure Switch Access with TACACS+ 124
Identifying the TACACS+ Server Host and Setting the Authentication Key 124
Configuring TACACS+ Login Authentication 125
Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services 128
Starting TACACS+ Accounting 129
Establishing a Session with a Router if the AAA Server is Unreachable 131
Monitoring TACACS+ 131
Additional References For Switch Access with TACACS+ 131
Feature Information for TACACS+ 132

**CHAPTER 8**

Configuring RADIUS 133
Prerequisites for Configuring RADIUS 133
Restrictions for Configuring RADIUS 134
Information about RADIUS 134
   RADIUS and Switch Access 134
   RADIUS Overview 134
   RADIUS Operation 135
   RADIUS Change of Authorization 136
      Change-of-Authorization Requests 137
      CoA Request Response Code 139
      CoA Request Commands 140
      Stacking Guidelines for Session Termination 142
Default RADIUS Configuration 143
RADIUS Server Host 143
RADIUS Login Authentication 144
AAA Server Groups 144
AAA Authorization 144
RADIUS Accounting 144
Vendor-Specific RADIUS Attributes 145
Vendor-Proprietary RADIUS Server Communication 156
How to Configure RADIUS 156
Identifying the RADIUS Server Host 156
Configuring RADIUS Login Authentication 159
Defining AAA Server Groups 161
Configuring RADIUS Authorization for User Privileged Access and Network Services 163
Starting RADIUS Accounting 164
Configuring Settings for All RADIUS Servers 165
Configuring the Device to Use Vendor-Specific RADIUS Attributes 167
Configuring the Device for Vendor-Proprietary RADIUS Server Communication 168
Configuring CoA on the Device 169
Monitoring CoA Functionality 171
Feature Information for RADIUS 172

CHAPTER 9

Configuring Kerberos 173
Prerequisites for Controlling Switch Access with Kerberos 173
Information about Kerberos 173
  Kerberos and Switch Access 174
  Kerberos Overview 174
  Kerberos Operation 176
    Authenticating to a Boundary Switch 176
    Obtaining a TGT from a KDC 176
    Authenticating to Network Services 177
  How to Configure Kerberos 177
Monitoring the Kerberos Configuration 177
Additional References 177
Feature Information for Kerberos 178

CHAPTER 10

MACsec Encryption 179
Restrictions for MACsec Encryption 179
Information about MACsec Encryption 179
  Media Access Control Security and MACsec Key Agreement 180
    MKA Policies 181
    Virtual Ports 181
    MKA Statistics 181
    MACsec, MKA and 802.1x Host Modes 181
  Information About MACsec MKA using EAP-TLS 182
CHAPTER 11 Configuring Secure Shell 221
Prerequisites for Configuring Secure Shell 221
Restrictions for Configuring Secure Shell 222
Information About Configuring Secure Shell 222
SSH And Switch Access 222
SSH Servers, Integrated Clients, and Supported Versions 222
SSH Configuration Guidelines 223
Secure Copy Protocol Overview 223
Secure Copy Protocol 224
How to Configure Secure Shell 224
Setting Up the Device to Run SSH 224
Configuring the SSH Server 225
Monitoring the SSH Configuration and Status 228
Feature Information for Secure Shell 228

CHAPTER 12 Configuring SSH File Transfer Protocol 229
Prerequisites for SSH File Transfer Protocol 229
Restrictions for SSH File Transfer Protocol 229
Information About SSH File Transfer Protocol 229
How to Configure SSH File Transfer Protocol 230
Configuring SFTP 230
Perform an SFTP Copy Operation 231
Example: Configuring SSH File Transfer Protocol 231
Additional References 231
Feature Information for SSH File Transfer Protocol 232

CHAPTER 13 X.509v3 Certificates for SSH Authentication 233
X.509v3 Certificates for SSH Authentication 233
Prerequisites for X.509v3 Certificates for SSH Authentication 233
Restrictions for X.509v3 Certificates for SSH Authentication 233
IPv6 ACLs Overview 297
Switch Stacks and IPv6 ACLs 298
ACL Precedence 298
VLAN Maps 298
Interactions with Other Features and Switches 299
Restrictions for IPv6 ACLs 299
Default Configuration for IPv6 ACLs 300
Configuring IPv6 ACLs 300
Attaching an IPv6 ACL to an Interface 304
Configuring VLAN Maps 305
Applying a VLAN Map to a VLAN 306
Monitoring IPv6 ACLs 307
Feature Information for IPv6 ACLs 308

CHAPTER 17 Configuring DHCP 309
Information About DHCP 309
DHCP Server 309
DHCP Relay Agent 309
DHCP Snooping 309
Option-82 Data Insertion 311
Cisco IOS DHCP Server Database 313
DHCP Snooping Binding Database 314
DHCP Snooping and Switch Stacks 315
How to Configure DHCP Features 315
Default DHCP Snooping Configuration 315
DHCP Snooping Configuration Guidelines 316
Configuring the DHCP Server 316
DHCP Server and Switch Stacks 316
Configuring the DHCP Relay Agent 317
Specifying the Packet Forwarding Address 318
Prerequisites for Configuring DHCP Snooping and Option 82 319
Enabling the Cisco IOS DHCP Server Database 320
Monitoring DHCP Snooping Information 321
Configuring DHCP Server Port-Based Address Allocation 321
CHAPTER 18  DHCPv6 Options Support  327
  Information About DHCPv6 Options Support  327
    CAPWAP Access Controller DHCPv6 Option  327
    DNS Search List Option  328
    DHCPv6 Client Link-Layer Address Option  328
    DHCPv6 Relay Agent  328
  How to Configure DHCPv6 Options Support  329
    Configuring CAPWAP Access Points  329
    Configuring DNS Search List Using IPv6 Router Advertisement Options  329
  Configuration Examples for DHCPv6 Options Support  331
    Example: Configuring CAPWAP Access Points  331
  Verifying DHCPv6 Options Support  331
  Feature Information for DHCPv6 Options Support  333

CHAPTER 19  Configuring IP Source Guard  335
  Information About IP Source Guard  335
    IP Source Guard  335
    IP Source Guard for Static Hosts  335
    IP Source Guard Configuration Guidelines  336
  How to Configure IP Source Guard  337
    Enabling IP Source Guard  337
    Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port  338
  Monitoring IP Source Guard  339
  Additional References  340
  Feature Information for IP Source Guard  340
Example: Programmatically Enabling SISF-Based Device Tracking in Cisco IOS XE Everest 16.9.x and Later Releases 399
Example: Disabling IPv6 Device Tracking on a Target 401
Example: Enabling IPv6 for SVI on VLAN (To Mitigate the Duplicate Address Problem) 401
Example: Mitigating the IPv4 Duplicate Address Problem 402
Example: Avoiding a Short Device-Tracking Binding Reachable Time 403
Feature History and Information for SISF-Based Device Tracking 403

CHAPTER 23

Configuring IEEE 802.1x Port-Based Authentication 405
Information About 802.1x Port-Based Authentication 405
Port-Based Authentication Process 406
Port-Based Authentication Initiation and Message Exchange 408
Authentication Manager for Port-Based Authentication 409
Port-Based Authentication Methods 409
Per-User ACLs and Filter-Ids 410
Port-Based Authentication Manager CLI Commands 411
Ports in Authorized and Unauthorized States 412
Port-Based Authentication and Switch Stacks 413
802.1x Host Mode 414
802.1x Multiple Authentication Mode 414
Multi-auth Per User VLAN assignment 415
MAC Move 416
MAC Replace 416
802.1x Accounting 417
802.1x Accounting Attribute-Value Pairs 417
802.1x Readiness Check 418
Switch-to-RADIUS-Server Communication 419
802.1x Authentication with VLAN Assignment 419
802.1x Authentication with Per-User ACLs 420
802.1x Authentication with Downloadable ACLs and Redirect URLs 421
VLAN ID-Based MAC Authentication 423
802.1x Authentication with Guest VLAN 423
802.1x Authentication with Restricted VLAN 424
802.1x Authentication with Inaccessible Authentication Bypass 425
Changing the Switch-to-Client Retransmission Time 452
Setting the Switch-to-Client Frame-Retransmission Number 453
Setting the Re-Authentication Number 454
Enabling MAC Move 455
Enabling MAC Replace 456
Configuring 802.1x Accounting 457
Configuring a Guest VLAN 459
Configuring a Restricted VLAN 460
  Configuring Number of Authentication Attempts on a Restricted VLAN 461
Configuring 802.1x Inaccessible Authentication Bypass with Critical Voice VLAN 462
  Example of Configuring Inaccessible Authentication Bypass 465
Configuring 802.1x Authentication with WoL 466
Configuring MAC Authentication Bypass 467
Configuring 802.1x User Distribution 468
  Example of Configuring VLAN Groups 468
Configuring NAC Layer 2 802.1x Validation 469
Configuring an Authenticator Switch with NEAT 471
Configuring a Supplicant Switch with NEAT 473
Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs 475
  Configuring Downloadable ACLs 475
  Configuring a Downloadable Policy 476
Configuring VLAN ID-based MAC Authentication 478
Configuring Flexible Authentication Ordering 479
Configuring Open1x 480
Disabling 802.1x Authentication on the Port 482
  Resetting the 802.1x Authentication Configuration to the Default Values 483
Monitoring 802.1x Statistics and Status 484
Feature Information for IEEE 802.1x Port-Based Authentication 484

CHAPTER 24

Web-Based Authentication 485
Web-Based Authentication Overview 485
  Device Roles 486
  Host Detection 487
  Session Creation 487
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Storm Control and Threshold Levels</td>
<td>509</td>
</tr>
<tr>
<td>Configuring Small-Frame Arrival Rate</td>
<td>511</td>
</tr>
<tr>
<td>Information About Protected Ports</td>
<td>513</td>
</tr>
<tr>
<td>Protected Ports</td>
<td>513</td>
</tr>
<tr>
<td>Default Protected Port Configuration</td>
<td>514</td>
</tr>
<tr>
<td>Protected Ports Guidelines</td>
<td>514</td>
</tr>
<tr>
<td>How to Configure Protected Ports</td>
<td>514</td>
</tr>
<tr>
<td>Configuring a Protected Port</td>
<td>514</td>
</tr>
<tr>
<td>Monitoring Protected Ports</td>
<td>515</td>
</tr>
<tr>
<td>Information About Port Blocking</td>
<td>515</td>
</tr>
<tr>
<td>Port Blocking</td>
<td>515</td>
</tr>
<tr>
<td>How to Configure Port Blocking</td>
<td>516</td>
</tr>
<tr>
<td>Blocking Flooded Traffic on an Interface</td>
<td>516</td>
</tr>
<tr>
<td>Monitoring Port Blocking</td>
<td>517</td>
</tr>
<tr>
<td>Prerequisites for Port Security</td>
<td>517</td>
</tr>
<tr>
<td>Restrictions for Port Security</td>
<td>517</td>
</tr>
<tr>
<td>Information About Port Security</td>
<td>518</td>
</tr>
<tr>
<td>Port Security</td>
<td>518</td>
</tr>
<tr>
<td>Types of Secure MAC Addresses</td>
<td>518</td>
</tr>
<tr>
<td>Sticky Secure MAC Addresses</td>
<td>518</td>
</tr>
<tr>
<td>Security Violations</td>
<td>518</td>
</tr>
<tr>
<td>Port Security Aging</td>
<td>520</td>
</tr>
<tr>
<td>Port Security and Switch Stacks</td>
<td>520</td>
</tr>
<tr>
<td>Default Port Security Configuration</td>
<td>520</td>
</tr>
<tr>
<td>Port Security Configuration Guidelines</td>
<td>520</td>
</tr>
<tr>
<td>Overview of Port-Based Traffic Control</td>
<td>522</td>
</tr>
<tr>
<td>How to Configure Port Security</td>
<td>522</td>
</tr>
<tr>
<td>Configuration Examples for Port Security</td>
<td>529</td>
</tr>
<tr>
<td>Information About Protocol Storm Protection</td>
<td>530</td>
</tr>
<tr>
<td>Protocol Storm Protection</td>
<td>530</td>
</tr>
<tr>
<td>Default Protocol Storm Protection Configuration</td>
<td>530</td>
</tr>
<tr>
<td>How to Configure Protocol Storm Protection</td>
<td>530</td>
</tr>
<tr>
<td>Enabling Protocol Storm Protection</td>
<td>530</td>
</tr>
<tr>
<td>Monitoring Protocol Storm Protection</td>
<td>531</td>
</tr>
</tbody>
</table>
CHAPTER 26  Configuring Control Plane Policing  533
  Restrictions for CoPP  533
  Information About Control Plane Policing  534
    CoPP Overview  534
    System-Defined Aspects of CoPP  534
    User-Configurable Aspects of CoPP  537
  How to Configure CoPP  538
    Enabling a CPU Queue or Changing the Policer Rate  538
    Disabling a CPU Queue  539
    Setting the Default Policer Rates for All CPU Queues  540
    Creating A User-Defined Class Map  541
  Examples for Configuring CoPP  543
    Example: Enabling a CPU Queue or Changing the Policer Rate of a CPU Queue  543
    Example: Disabling a CPU Queue  544
    Example: Setting the Default Policer Rates for All CPU Queues  544
    Example: Creating a User-Defined Class Map  546
  Monitoring CoPP  547
  Feature History for Control Plane Policing  548

CHAPTER 27  Configuring Authorization and Revocation of Certificates in a PKI  549
  Configuring Authorization and Revocation of Certificates in a PKI  549
  Prerequisites for Authorization and Revocation of Certificates  549
  Restrictions for Authorization and Revocation of Certificates  550
  Information About Authorization and Revocation of Certificates  550
    PKI Authorization  550
    PKI and AAA Server Integration for Certificate Status  550
    CRLs or OCSP Server Choosing a Certificate Revocation Mechanism  552
    When to Use Certificate-Based ACLs for Authorization or Revocation  554
    PKI Certificate Chain Validation  556
  How to Configure Authorization and Revocation of Certificates for Your PKI  556
    Configuring PKI Integration with a AAA Server  556
CHAPTER 1

Preventing Unauthorized Access

- Finding Feature Information, on page 1
- Preventing Unauthorized Access, on page 1
- Feature Information for Preventing Unauthorized Access, on page 2

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.

Feature Information for Preventing Unauthorized Access

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventing Unauthorized Access</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>You can prevent unauthorized users from reconfiguring your switch and viewing configuration information.</td>
</tr>
</tbody>
</table>
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.

- Password type 0 and type 7 are deprecated. So password type 0 and type 7, used for administrator login to Console, Telnet, SSH, webUI, and NETCONF, must be migrated to password type 8 or type 9.

- No action is required if username and password are type 0 and type 7 for local authentication such as CHAP, EAP and so on for ISG and Dot1x.

- Enable password type 0 and type 7 must be migrated to password type 8 or type 9.

- Password type 5 is deprecated. Password type 5 must be migrated to stronger password type 8 or type 9.
Information About Passwords and Privilege Levels

Default Password and Privilege Level Configuration

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

This table shows the default password and privilege level configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable password and privilege level</td>
<td>No password is defined. The default is level 15 (privileged EXEC level). The password is not encrypted in the configuration file.</td>
</tr>
<tr>
<td>Enable secret password and privilege level</td>
<td>No password is defined. The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.</td>
</tr>
<tr>
<td>Line password</td>
<td>No password is defined.</td>
</tr>
</tbody>
</table>

Additional Password Security

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, you can use either the enable password or enable secret global configuration commands. Both commands accomplish the same thing; that is, you can establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify.

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

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

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

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.

**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.

**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.

**Privilege Levels**

Cisco devices use privilege levels to provide password security for different levels of switch operation. By default, the Cisco IOS software operates in two modes (privilege levels) of password security: user EXEC (Level 1) and privileged EXEC (Level 15). You can configure up to 16 hierarchical levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

**Privilege Levels on Lines**

Users can override the privilege level you set using the `privilege level` line configuration command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the `disable` command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level. You might specify a high level or privilege level for your console line to restrict line usage.

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

**Command Privilege Levels**

When you set a command to a privilege level, all commands whose syntax is a subset of that command are also set to that level. For example, if you set the `show ip traffic` command to level 15, the `show` commands and `show ip` commands are automatically set to privilege level 15 unless you set them individually to different levels.
# How to Control Switch Access with Passwords and Privilege Levels

## Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode. Follow these steps to set or change a static enable password:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
   Example:  
   Device> enable |
| **Step 2** configure terminal | Enters global configuration mode.  
   Example:  
   Device# configure terminal |
| **Step 3** enable password password | Defines a new password or changes an existing password for access to privileged EXEC mode.  
   By default, no password is defined.  
   For `password`, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password abc?123, do this:  
   1. Enter abc.  
   2. Enter Ctrl-v.  
   3. Enter ?123.  
   When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter abc?123 at the password prompt.  
   Example:  
   Device(config)# enable password secret321 |

---

Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)
### Protecting Enable and Enable Secret Passwords with Encryption

Follow these steps to establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Use one of the following:</td>
<td>• Defines a new password or changes an existing password for access to privileged EXEC mode.</td>
</tr>
<tr>
<td>• enable password [level level] {password encryption-type encrypted-password}</td>
<td>• Defines a secret password, which is saved using a nonreversible encryption method.</td>
</tr>
<tr>
<td>• enable secret [level level] {password encryption-type encrypted-password}</td>
<td>• (Optional) For level, the range is from 0 to 15. Level 1 is normal user EXEC</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>mode privileges. The default level is 15 (privileged EXEC mode privileges).</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# enable password example102</td>
</tr>
<tr>
<td>or</td>
<td>or</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# enable secret level 1 password secret123sample</td>
</tr>
<tr>
<td>For password, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.</td>
<td></td>
</tr>
<tr>
<td>(Optional) For encryption-type, only type 5, a Cisco proprietary encryption algorithm, is available. If you specify an encryption type, you must provide an encrypted password—an encrypted password that you copy from another switch configuration.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>If you specify an encryption type and then enter a clear text password, you cannot re-enter privileged EXEC mode. You cannot recover a lost encrypted password by any method.</td>
</tr>
<tr>
<td>Step 4</td>
<td>service password-encryption</td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Encrypts the password when the password is defined or when the configuration is written.</td>
</tr>
<tr>
<td>Example:</td>
<td>Encryption prevents the password from being readable in the configuration file.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show running-config</td>
</tr>
<tr>
<td>Example:</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Disabling Password Recovery

Follow these steps to disable password recovery to protect the security of your switch:

**Before you begin**

If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in VTP transparent mode, we recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, you can download the saved files to the switch by using the Xmodem protocol.

**Procedure**

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

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

| **Step 3**        |         |
| `system disable password recovery switch {all | <1-9>}` | Disables password recovery. |
| Example:           | • *all* - Sets the configuration on switches in stack. |
| | • *<1-9>* - Sets the configuration on the Switch Number selected. |
| `Device(config)# system disable password recovery switch all` | 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`             | Returns to privileged EXEC mode. |
| Example:          |         |
| `Device(config)# end` | |
What to do next

To remove disable password recovery, use the no system disable password recovery switch all global configuration command.

Setting a Telnet Password for a Terminal Line

Beginning in user EXEC mode, follow these steps to set a Telnet password for the connected terminal line:

Before you begin

- Attach a PC or workstation with emulation software to the switch console port, or attach a PC to the Ethernet management port.
- The default data characteristics of the console port are 9600, 8, 1, no parity. You might need to press the Return key several times to see the command-line prompt.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td>Note: If a password is required for access to privileged EXEC mode, you will be prompted for it.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>line vty 0 15</td>
<td>Configures the number of Telnet sessions (lines), and enters line configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# line vty 0 15</td>
<td>There are 16 possible sessions on a command-capable Device. The 0 and 15 mean that you are configuring all 16 possible Telnet sessions.</td>
</tr>
<tr>
<td>Step 4</td>
<td>password</td>
<td>Sets a Telnet password for the line or lines.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-line)# password abcxyz543</td>
<td>For password, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
**Configuring Username and Password Pairs**

Follow these steps to configure username and password pairs:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>username name [privilege level] {password encryption-type password}</code></td>
<td>Sets the username, privilege level, and password for each user.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>- For <em>name</em>, specify the user ID as one word or the MAC address. Spaces and quotation marks are not allowed.</td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# username adamsample privilege 1 password secret456</code></td>
<td>- You can configure a maximum of 12000 clients each, for both username and MAC filter.</td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# username 111111111111 mac attribute</code></td>
<td>- (Optional) For <em>level</em>, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged access.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>• For encryption-type, enter 0 to specify that an unencrypted password will follow. Enter 7 to specify that a hidden password will follow. • For password, specify the password the user must enter to gain access to the Device. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Step 4** | Use one of the following:  
  • line console 0  
  • line vty 0 15  
  **Example:**  
  Device(config)# line console 0  
  or  
  Device(config)# line vty 15  
  Enters line configuration mode, and configures the console port (line 0) or the VTY lines (line 0 to 15). |
| **Step 5** | login local  
  **Example:**  
  Device(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:**  
  Device(config)# end  
  Returns to privileged EXEC mode. |
| **Step 7** | show running-config  
  **Example:**  
  Device# show running-config  
  Verifies your entries. |
| **Step 8** | copy running-config startup-config  
  **Example:**  
  Device# copy running-config startup-config  
  (Optional) Saves your entries in the configuration file. |
### Setting the Privilege Level for a Command

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

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>privilege mode level level command</td>
<td>Sets the privilege level for a command.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>• For mode, enter configure for global configuration mode, exec for EXEC mode, interface for interface configuration mode, or line for line configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Device(config)# privilege exec level 14 configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>enable password level level password</td>
<td>Specifies the password to enable the privilege level.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>• For level, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges.</td>
</tr>
<tr>
<td></td>
<td>Device(config)# enable password level 14 SecretPswd14</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Changing the Default Privilege Level for Lines

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

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>line vty line</code></td>
<td>Selects the virtual terminal line on which to restrict access.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# line vty 10</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>privilege level level</code></td>
<td>Changes the default privilege level for the line.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# privilege level 15</code></td>
<td>For <em>level</em>, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the <code>enable</code> password.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose
--- | ---
Step 6 `copy running-config startup-config` | (Optional) Saves your entries in the configuration file.

### Example:

```
Device# copy running-config startup-config
```

### 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.

### Loggin 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.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable level</code></td>
<td>Logs in to a specified privilege level. Following the example, Level 15 is privileged EXEC mode. For <code>level</code>, the range is 0 to 15.</td>
</tr>
<tr>
<td>Example: <code>Device&gt; enable 15</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>disable level</code></td>
<td>Exits to a specified privilege level. Following the example, Level 1 is user EXEC mode. For <code>level</code>, the range is 0 to 15.</td>
</tr>
<tr>
<td>Example: <code>Device# disable 1</code></td>
<td></td>
</tr>
</tbody>
</table>

### Monitoring Switch Access

#### Table 3: Commands for Displaying DHCP Information

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show privilege</code></td>
<td>Displays the privilege level configuration.</td>
</tr>
</tbody>
</table>
Configuration Examples for Setting Passwords and Privilege Levels

Example: Setting or Changing a Static Enable Password

This example shows how to change the enable password to 1lu2c3k4y5. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

Device(config)# enable password 1lu2c3k4y5

Example: Protecting Enable and Enable Secret Passwords with Encryption

This example shows how to configure the encrypted password $1$FaDO$Xyti5Rkl3LoyxzS8 for privilege level 2:

Device(config)# enable secret level 2 5 $1$FaDO$Xyti5Rkl3LoyxzS8

Example: Setting a Telnet Password for a Terminal Line

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

Device(config)# line vty 10
Device(config-line)# password let45me67in89

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:

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

Additional References

Error Message Decoder

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

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

Technical Assistance

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

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

Feature Information for Controlling Switch Access with Passwords and Privileges

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support.

To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlling Switch Access with Passwords and Privileges</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>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.</td>
</tr>
</tbody>
</table>
CHAPTER 3

Configuring Authentication

Authentication provides a method to identify users, which includes the login and password dialog, challenge and response, messaging support, and encryption, depending on the selected security protocol. Authentication is the way a user is identified prior to being allowed access to the network and network services.

- Prerequisites for Configuring Authentication, on page 19
- Restrictions for Configuring Authentication, on page 19
- Information About Configuring Authentication, on page 20
- How to Configure AAA Authentication Methods, on page 27
- Additional References for Configuring Authentication, on page 72
- Feature Information for Configuring Authentication, on page 73

Prerequisites for Configuring Authentication

The Cisco software implementation of authentication is divided into Authentication, Authorization, and Accounting (AAA) authentication and nonauthentication methods. Cisco recommends that, whenever possible, AAA security services be used to implement authentication.

Restrictions for Configuring Authentication

- The number of AAA method lists that can be configured is 250.
- If you configure one RADIUS server with the nonstandard option and another RADIUS server without the nonstandard option, the RADIUS-server host with the nonstandard option does not accept a predefined host. If you configure the same RADIUS server host IP address for a different UDP destination port for accounting requests by using the `acct-port` keyword and a UDP destination port for authentication requests by using the `auth-port` keyword with and without the nonstandard option, the RADIUS server does not accept the nonstandard option.
Information About Configuring Authentication

Named Method Lists for Authentication

A named list of authentication methods is first defined before AAA authentication can be configured, and the named list is then applied to various interfaces. The method list defines the types of authentication and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which is named "default"). The default method list is automatically applied to all interfaces, except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list is a sequential list describing the authentication methods to be queried to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. Cisco software uses the first listed method to authenticate users. If that method fails to respond, the Cisco software selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method, or all methods defined in the method list are exhausted.

Note that the Cisco software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle, that is, the security server or local username database responds by denying the user access, then the authentication process stops and no other authentication methods are attempted.

Method Lists and Server Groups

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers and T1 and T2 are TACACS+ servers. R1 and R2 make up the group of RADIUS servers. T1 and T2 make up the group of TACACS+ servers.

Figure 1: Typical AAA Network Configuration
Using server groups, you can specify a subset of the configured server hosts and use them for a particular service. For example, server groups allow you to define R1 and R2 as a server group, and define T1 and T2 as a separate server group. For example, you can specify R1 and T1 in the method list for authentication login, while specifying R2 and T2 in the method list for PPP authentication.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different 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 failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order in which they are configured.)

For more information about configuring server groups and about configuring server groups based on Dialed Number Identification Service (DNIS) numbers, refer to the “Configuring RADIUS” or “Configuring TACACS+” chapter.

**Method List Examples**

Suppose the system administrator has decided on a security solution where all interfaces will use the same authentication methods to authenticate PPP connections. In the RADIUS group, R1 is contacted first for authentication information, then if there is no response, R2 is contacted. If R2 does not respond, T1 in the TACACS+ group is contacted; if T1 does not respond, T2 is contacted. If all designated servers fail to respond, authentication falls to the local username database on the access server itself. To implement this solution, the system administrator would create a default method list by entering the following command:

```
aaa authentication ppp default group radius group tacacs+ local
```

In this example, “default” is the name of the method list. The protocols included in this method list are listed after the name, in the order they are to be queried. The default list is automatically applied to all interfaces.

When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern would continue through the remaining designated methods until the user is either authenticated or rejected, or until the session is terminated.

It is important to remember that a FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

Suppose the system administrator wants to apply a method list only to a particular interface or set of interfaces. In this case, the system administrator creates a named method list and then applies this named list to the applicable interfaces. The following example shows how the system administrator can implement an authentication method that will be applied only to interface 3:

```
aaa authentication ppp default group radius group tacacs+ local
aaa authentication ppp apple group radius group tacacs+ local none
   interface async 3
   ppp authentication chap apple
```
In this example, “apple” is the name of the method list, and the protocols included in this method list are listed after the name in the order in which they are to be performed. After the method list has been created, it is applied to the appropriate interface. Note that the method list name (apple) in both the AAA and PPP authentication commands must match.

In the following example, the system administrator uses server groups to specify that only R2 and T2 are valid servers for PPP authentication. To do this, the administrator must define specific server groups whose members are R2 (172.16.2.7) and T2 (172.16.2.77), respectively. In this example, the RADIUS server group “rad2only” is defined as follows using the `aaa group server` command:

```
aaa group server radius rad2only
  server 172.16.2.7
```

The TACACS+ server group “tac2only” is defined as follows using the `aaa group server` command:

```
aaa group server tacacs+ tac2only
  server 172.16.2.77
```

The administrator then applies PPP authentication using the server groups. In this example, the default methods list for PPP authentication follows this order: `group rad2only`, `group tac2only`, and `local`:

```
aaa authentication ppp default group rad2only group tac2only local
```

If a method list is configured under VTY lines, the corresponding method list must be added to AAA. The following example shows how to configure a method list under a VTY line:

```
Device# configure terminal
Device(config)# line vty 0 4
Device(config)# authorization commands 15 auth1
```

The following example shows how to configure a method list in AAA:

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 auth1 group tacacs+
```

If no method list is configured under VTY lines, the default method list must be added to AAA. The following example shows a VTY configuration without a method list:

```
Device# configure terminal
Device(config)# line vty 0 4
```

The following example shows how to configure the default method list:

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 default group tacacs+
```

### About RADIUS Change of Authorization

A standard RADIUS interface is typically used in a pulled model, in which the request originates from a device attached to a network and the response is sent from the queried servers. The Cisco software supports the RADIUS CoA request defined in RFC 5176 that is used in a pushed model, in which the request originates from the external server to the device attached to the network, and enables the dynamic reconfiguring of sessions from external authentication, authorization, and accounting (AAA) or policy servers.
Use the following per-session CoA requests:

- Session reauthentication
- Session termination
- Session termination with port shutdown
- Session termination with port bounce
- Security and Password
- Accounting

### CoA Requests

CoA requests, as described in RFC 5176, are used in a pushed model to allow for session identification, host reauthentication, and session termination. The model comprises 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 device 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 device for a session termination.

The following table shows the IETF attributes that are supported for the RADIUS Change of Authorization (CoA) feature.

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>Attribute Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>State</td>
</tr>
<tr>
<td>31</td>
<td>Calling-Station-ID</td>
</tr>
<tr>
<td>44</td>
<td>Acct-Session-ID</td>
</tr>
<tr>
<td>80</td>
<td>Message-Authenticator</td>
</tr>
<tr>
<td>101</td>
<td>Error-Cause</td>
</tr>
</tbody>
</table>

The following table shows the possible values for the Error-Cause attribute.

<table>
<thead>
<tr>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Residual Session Context Removed</td>
</tr>
</tbody>
</table>
CoA Request Response Code

The CoA Request Response code can be used to issue a command to the device. The supported commands are listed in the “CoA Request Commands” section.

The packet format for a CoA Request Response code as defined in RFC 5176 consists of the following fields: Code, Identifier, Length, Authenticator, and Attributes in the Type:Length:Value (TLV) format.

The Attributes field is used to carry Cisco VSAs.

### Session Identification

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

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

Unless all session identification attributes included in the CoA message match the session, the device returns a Disconnect-NAK or CoA-NAK with the “Invalid Attribute Value” error-code attribute.

<table>
<thead>
<tr>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>202</td>
<td>Invalid EAP Packet (Ignored)</td>
</tr>
<tr>
<td>401</td>
<td>Unsupported Attribute</td>
</tr>
<tr>
<td>402</td>
<td>Missing Attribute</td>
</tr>
<tr>
<td>403</td>
<td>NAS Identification Mismatch</td>
</tr>
<tr>
<td>404</td>
<td>Invalid Request</td>
</tr>
<tr>
<td>405</td>
<td>Unsupported Service</td>
</tr>
<tr>
<td>406</td>
<td>Unsupported Extension</td>
</tr>
<tr>
<td>407</td>
<td>Invalid Attribute Value</td>
</tr>
<tr>
<td>501</td>
<td>Administratively Prohibited</td>
</tr>
<tr>
<td>502</td>
<td>Request Not Routable (Proxy)</td>
</tr>
<tr>
<td>503</td>
<td>Session Context Not Found</td>
</tr>
<tr>
<td>504</td>
<td>Session Context Not Removable</td>
</tr>
<tr>
<td>505</td>
<td>Other Proxy Processing Error</td>
</tr>
<tr>
<td>506</td>
<td>Resources Unavailable</td>
</tr>
<tr>
<td>507</td>
<td>Request Initiated</td>
</tr>
<tr>
<td>508</td>
<td>Multiple Session Selection Unsupported</td>
</tr>
</tbody>
</table>
A CoA NAK message is not sent for all CoA requests with a key mismatch. The message is sent only for the first three requests for a client. After that, all the packets from that client are dropped. When there is a key mismatch, the response authenticator sent with the CoA NAK message is calculated from a dummy key value.

CoA ACK Response Code

If an authorization state is changed successfully, a positive acknowledgment (ACK) is sent. The attributes returned within a CoA ACK can vary based on the CoA Request.

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.

CoA Request Commands

The commands supported on the device are shown in the table below. All CoA commands must include the session identifier between the device and the CoA client.

Table 7: CoA Request Commands Supported on the Device

<table>
<thead>
<tr>
<th>Command</th>
<th>Cisco VSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bounce host port</td>
<td>Cisco:Avpair=&quot;subscriber:command=bounce-host-port&quot;</td>
</tr>
<tr>
<td>Disable host port</td>
<td>Cisco:Avpair=&quot;subscriber:command=disable-host-port&quot;</td>
</tr>
<tr>
<td>Reauthenticate host</td>
<td>Cisco:Avpair=&quot;subscriber:command=reauthenticate&quot;</td>
</tr>
<tr>
<td>Terminate session</td>
<td>This is a standard disconnect request that does not require a VSA</td>
</tr>
</tbody>
</table>

Session Reauthentication

To initiate session reauthentication, the authentication, authorization, and accounting (AAA) server sends a standard CoA-Request message that contains a Cisco VSA and one or more session identification attributes. The Cisco VSA is in the form of Cisco:Avpair="subscriber:command=reauthenticate".

The current session state determines the device’s response to the message in the following scenarios:

- If the session is currently authenticated by IEEE 802.1x, the device responds by sending an Extensible Authentication Protocol over LAN (EAPoL)-RequestId message to the server.
- If the session is currently authenticated by MAC authentication bypass (MAB), the device 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 device receives the command, the device terminates the process and restarts the authentication sequence, starting with the method configured to be attempted first.
Session Termination

A CoA Disconnect-Request terminates the session without disabling the host port. CoA Disconnect-Request termination causes reinitialization of the authenticator state machine for the specified host, but does not restrict the host’s access to the network. If the session cannot be located, the device returns a Disconnect-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the device terminates the session. After the session has been completely removed, the device returns a Disconnect-ACK message.

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 cause problems on the network and network access needs to be immediately blocked for the host. If you want to restore network access on the port, reenable it using a non-RADIUS mechanism.

CoA Request Disable Host Port

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. If you want to restore network access on the port, reenable it using a non-RADIUS mechanism. This command is carried in a standard CoA-Request message that has the following VSA:

Cisco:Avpair="subscriber:command=disable-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the “Session Identification” section. If the device cannot locate the session, it returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the device locates the session, it disables the hosting port and returns a CoA-ACK message.

If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is re-sent from the client. If the device fails after returning a CoA-ACK message to the client but before the operation is complete, the operation is restarted on the new active device.

To ignore the RADIUS server CoA disable port command, see the “Configuring the Device to Ignore Bounce and Disable RADIUS CoA Requests” section.

CoA Request Bounce Port

A RADIUS server CoA bounce port sent from a RADIUS server can cause a link flap on an authentication port, which triggers DHCP renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer) that does not have a mechanism to detect a change on this authentication port. The CoA bounce port is carried in a standard CoA-Request message that contains the following VSA:

Cisco:Avpair="subscriber:command=bounce-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the Session Identification. If the session cannot be located, the device returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the device disables the hosting port for a period of 10 seconds, reenables it (port-bounce), and returns a CoA-ACK.

To ignore the RADIUS server CoA bounce port, see the “Configuring the Device to Ignore Bounce and Disable RADIUS CoA Requests” section.
Domain Stripping

You can remove the domain name from the username received at the global level by using the `radius-server domain-stripping` command. When the `radius-server domain-stripping` command is configured, all the AAA requests with “user@example.com” go to the remote RADIUS server with the reformatted username “user.” The domain name is removed from the request.

Note

Domain stripping will not be done in a TACACS configuration.

The AAA Broadcast Accounting feature allows accounting information to be sent to multiple AAA servers at the same time, that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows you to send accounting information to private and public AAA servers. It also provides redundant billing information for voice applications.

The Domain Stripping feature allows domain stripping to be configured at the server group level.

Per-server group configuration overrides the global configuration. If domain stripping is not enabled globally, but it is enabled in a server group, then it is enabled only for that server group. Also, if virtual routing and forwarding (VRF)-specific domain stripping is configured globally and in a server group for a different VRF, domain stripping is enabled in both the VRFs. VRF configurations are taken from server-group configuration mode. If server-group configurations are disabled in global configuration mode but are available in server-group configuration mode, all configurations in server-group configuration mode are applicable.

After the domain stripping and broadcast accounting are configured, you can create separate accounting records as per the configurations.

How to Configure AAA Authentication Methods

Configuring Login Authentication Using AAA

The AAA security services facilitate a variety of login authentication methods. Use the `aaa authentication login` command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the `aaa authentication login` command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the `login authentication` line configuration command.

To configure login authentication by using AAA, use the following commands beginning in global configuration mode:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Router(config)# <code>aaa new-model</code></td>
<td>Enables AAA globally.</td>
</tr>
<tr>
<td>Step 2 Router(config)# `aaa authentication login [default</td>
<td>list-name] method1 [method2 ...]`</td>
</tr>
<tr>
<td>Step 3 Router(config)# `line [aux</td>
<td>console</td>
</tr>
</tbody>
</table>
Configuring Login Authentication Using AAA

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4 Router(config-line)# login authentication</td>
<td>Applies the authentication list to a line or set of lines.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>{default</td>
<td>list-name}</td>
</tr>
</tbody>
</table>

What to do next

The list-name is a character string used to name the list you are creating. The method argument refers to 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. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line.

For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, enter the following command:

```
aaa authentication login default group tacacs+ none
```

**Note**

Because the none keyword enables any user logging in to successfully authenticate, it should be used only as a backup method of authentication.

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

For example, to specify RADIUS as the default method for user authentication during login, enter the following command:

```
aaa authentication login default group radius
```

The table below lists the supported login authentication methods.

**Table 8: AAA Authentication Login Methods**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>krb5</td>
<td>Uses Kerberos 5 for authentication.</td>
</tr>
<tr>
<td>krb5-telnet</td>
<td>Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router. If selected, this keyword must be listed as the first method in the method list.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>local-case</td>
<td>Uses case-sensitive local username authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
</tbody>
</table>
Use the list of all RADIUS servers for authentication.

- **group radius**

Use the list of all TACACS+ servers for authentication.

- **group tacacs+**

Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the group name.

- **group group-name**

The `login` command only changes username and privilege level but does not execute a shell; therefore autocommands will not be executed. To execute autocommands under this circumstance, you need to establish a Telnet session back into the router (loop-back). Make sure that the router has been configured for secure Telnet sessions if you choose to implement autocommands this way.

### Login Authentication Using Enable Password

Use the `aaa authentication login` command with the `enable method` keyword to specify the enable password as the login authentication method. For example, to specify the enable password as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default enable
```

Before you can use the enable password as the login authentication method, you need to define the enable password. For more information about defining enable passwords, refer to the chapter “Configuring Passwords and Privileges.”

### Login Authentication Using Kerberos

Authentication via Kerberos is different from most other authentication methods: the user’s password is never sent to the remote access server. Remote users logging in to the network are prompted for a username. If the key distribution center (KDC) has an entry for that user, it creates an encrypted ticket granting ticket (TGT) with the password for that user and sends it back to the router. The user is then prompted for a password, and the router attempts to decrypt the TGT with that password. If it succeeds, the user is authenticated and the TGT is stored in the user’s credential cache on the router.

While krb5 does use the KINIT program, a user does not need to run the KINIT program to get a TGT to authenticate to the router. This is because KINIT has been integrated into the login procedure in the Cisco IOS XE implementation of Kerberos.

Use the `aaa authentication login` command with the `krb5 method` keyword to specify Kerberos as the login authentication method. For example, to specify Kerberos as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default krb5
```

Before you can use Kerberos as the login authentication method, you need to enable communication with the Kerberos security server. For more information about establishing communication with a Kerberos server, refer to the chapter “Configuring Kerberos.”
Login Authentication Using Line Password

Use the `aaa authentication login` command with the `line method` keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default line
```

Before you can use a line password as the login authentication method, you need to define a line password. For more information about defining line passwords, refer to the Configuring Line Password Protection.

Login Authentication Using Local Password

Use the `aaa authentication login` command with the `local method` keyword to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default local
```

For information about adding users into the local username database, refer to the Establishing Username Authentication.

Login Authentication Using Group RADIUS

Use the `aaa authentication login` command with the `group radius` method to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default group radius
```

Before you can use RADIUS as the login authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.”

Configuring RADIUS Attribute 8 in Access Requests

After you have used the `aaa authentication login` command to specify RADIUS and your login host has been configured to request its IP address from the NAS, you can send attribute 8 (Framed-IP-Address) in access-request packets by using the `radius-server attribute 8 include-in-access-req` command in global configuration mode. This command makes it possible for NAS to provide the RADIUS server a hint of the user IP address in advance for user authentication. For more information about attribute 8, refer to the appendix “RADIUS Attributes” at the end of the book.

Login Authentication Using Group TACACS

Use the `aaa authentication login` command with the `group tacacs+` method to specify TACACS+ as the login authentication method. For example, to specify TACACS+ as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default group tacacs+
```
Before you can use TACACS+ as the login authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

**Login Authentication Using group group-name**

Use the `aaa authentication login` command with the `group group-name` method to specify a subset of RADIUS or TACACS+ servers to use as the login authentication method. To specify and define the group name and the members of the group, use the `aaa group server` command. For example, use the `aaa group server` command to first define the members of `group loginrad`:

```
aaa group server radius loginrad
  server 172.16.2.3
  server 172.16.2.17
  server 172.16.2.32
```

This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the group `loginrad`.

To specify `group loginrad` as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default group loginrad
```

Before you can use a group name as the login authentication method, you need to enable communication with the RADIUS or TACACS+ security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.” For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

**Configuring PPP Authentication Using AAA**

Many users access network access servers through dialup via async or ISDN. Dialup via async or ISDN bypasses the CLI completely; instead, a network protocol (such as PPP or ARA) starts as soon as the connection is established.

The AAA security services facilitate a variety of authentication methods for use on serial interfaces running PPP. Use the `aaa authentication ppp` command to enable AAA authentication no matter which of the supported PPP authentication methods you decide to use.

To configure AAA authentication methods for serial lines using PPP, use the following commands in global configuration mode:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Router(config)# <code>aaa new-model</code></td>
<td>Enables AAA globally.</td>
</tr>
<tr>
<td></td>
<td>`aaa authentication ppp [default</td>
<td>list-name] method1 method2...`</td>
</tr>
<tr>
<td></td>
<td>Router(config)# <code>interface interface-type interface-number</code></td>
<td>Enters interface configuration mode for the interface to which you want to apply the authentication list.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

Applies the authentication list to a line or set of lines. In this command, `protocol1` and `protocol2` represent the following protocols: CHAP, MS-CHAP, and PAP. PPP authentication is attempted first using the first authentication method, specified by `protocol1`. If `protocol1` is unable to establish authentication, the next configured protocol is used to negotiate authentication.

### Step 4

```plaintext
Router(config-if)# ppp authentication {protocol1 [protocol2]]} [if-needed] [default [list-name]} [callin] [one-time][optional]
```

### What to do next

With the `aaa authentication ppp` command, you create one or more lists of authentication methods that are tried when a user tries to authenticate via PPP. These lists are applied using the `ppp` authentication line configuration command.

To create a default list that is used when a named list is not specified in the `ppp authentication` command, use the `default` keyword followed by the methods you want used in default situations.

For example, to specify the local username database as the default method for user authentication, enter the following command:

```plaintext
aaa authentication ppp default local
```

The `list-name` is any character string used to name the list you are creating. The method argument refers to 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. To specify that the authentication should succeed even if all methods return an error, specify `none` as the final method in the command line.

For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, enter the following command:

```plaintext
aaa authentication ppp default group tacacs+ none
```

### Note

Because `none` allows all users logging in to authenticate successfully, it should be used as a backup method of authentication.

The table below lists the supported login authentication methods.

### Table 9: AAA Authentication PPP Methods

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>if-needed</td>
<td>Does not authenticate if user has already been authenticated on a TTY line.</td>
</tr>
<tr>
<td>krb5</td>
<td>Uses Kerberos 5 for authentication (can only be used for PAP authentication).</td>
</tr>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>local-case</td>
<td>Uses case-sensitive local username authentication.</td>
</tr>
</tbody>
</table>
PPP Authentication Using Kerberos

Use the `aaa authentication ppp` command with the `krb5` method keyword to specify Kerberos as the authentication method for use on interfaces running PPP. For example, to specify Kerberos as the method of user authentication when no other method list has been defined, enter the following command:

```
aaa authentication ppp default krb5
```

Before you can use Kerberos as the PPP authentication method, you need to enable communication with the Kerberos security server. For more information about establishing communication with a Kerberos server, refer to the chapter “Configuring Kerberos”.

---

**Note**

Kerberos login authentication works only with PPP PAP authentication.

PPP Authentication Using Local Password

Use the `aaa authentication ppp` command with the `method` keyword `local` to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of authentication for use on lines running PPP when no other method list has been defined, enter the following command:

```
aaa authentication ppp default local
```

For information about adding users into the local username database, refer to the Establishing Username Authentication.

PPP Authentication Using Group RADIUS

Use the `aaa authentication ppp` command with the `group radius` method to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication ppp default group radius
```

Before you can use RADIUS as the PPP authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.”

---

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>group radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>group tacacs+</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
<tr>
<td>group group-name</td>
<td>Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <code>aaa group server radius</code> or <code>aaa group server tacacs+</code> command.</td>
</tr>
</tbody>
</table>
Configuring RADIUS Attribute 44 in Access Requests

After you have used the `aaa authentication ppp` command with the `group radius` method to specify RADIUS as the login authentication method, you can configure your device to send attribute 44 (Acct-Session-ID) in access-request packets by using the `radius-server attribute 44 include-in-access-req` command in global configuration mode. This command allows the RADIUS daemon to track a call from the beginning to the end.

PPP Authentication Using Group TACACS

Use the `aaa authentication ppp` command with the `group tacacs+` method to specify TACACS+ as the login authentication method. For example, to specify TACACS+ as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication ppp default group tacacs+
```

Before you can use TACACS+ as the PPP authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

PPP Authentication Using group group-name

Use the `aaa authentication ppp` command with the `group group-name` method to specify a subset of RADIUS or TACACS+ servers to use as the login authentication method. To specify and define the group name and the members of the group, use the `aaa group server` command. For example, use the `aaa group server` command to first define the members of `group pprrad`:

```
aaa group server radius pprrad
  server 172.16.2.3
  server 172.16.2.17
  server 172.16.2.32
```

This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the group `ppprad`.

To specify `group pprrad` as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication ppp default group pprrad
```

Before you can use a group name as the PPP authentication method, you need to enable communication with the RADIUS or TACACS+ security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS”. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

Configuring AAA Scalability for PPP Requests

You can configure and monitor the number of background processes allocated by the PPP manager in the network access server (NAS) to deal with AAA authentication and authorization requests. The AAA Scalability feature enables you to configure the number of processes used to handle AAA requests for PPP, thus increasing the number of users that can be simultaneously authenticated or authorized.

To allocate a specific number of background processes to handle AAA requests for PPP, use the following command in global configuration mode:
Allocates a specific number of background processes to handle AAA authentication and authorization requests for PPP.

The argument *number* defines the number of background processes earmarked to process AAA authentication and authorization requests for PPP and can be configured for any value from 1 to 2147483647. Because of the way the PPP manager handles requests for PPP, this argument also defines the number of new users that can be simultaneously authenticated. This argument can be increased or decreased at any time.

Allocating additional background processes can be expensive. You should configure the minimum number of background processes capable of handling the AAA requests for PPP.

### Configuring ARAP Authentication Using AAA

Using the `aaa authentication arap` command, you can create one or more lists of authentication methods that are tried when AppleTalk Remote Access Protocol (ARAP) users attempt to log in to the device. These lists are used with the `arap authentication` line configuration command.

Use the following commands starting in global configuration mode:

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
</tr>
</tbody>
</table>

### What to do next

The *list-name* is any character string used to name the list you are creating. The *method* argument refers to the actual list of methods the authentication algorithm tries, in the sequence entered.
To create a default list that is used when a named list is not specified in the `arap authentication` command, use the `default` keyword followed by the methods you want to use in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify `none` as the final method in the command line.

---

**Note**

Because `none` allows all users logging in to be authenticated, it should be used as a backup method of authentication.

The following table lists the supported login authentication methods.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-guest</td>
<td>Allows guest logins only if the user has already logged in to EXEC mode.</td>
</tr>
<tr>
<td>guest</td>
<td>Allows guest logins.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>local-case</td>
<td>Uses case-sensitive local username authentication.</td>
</tr>
<tr>
<td>group radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>group tacacs+</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
<tr>
<td>group group-name</td>
<td>Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <code>aaa group server radius</code> or <code>aaa group server tacacs+</code> command.</td>
</tr>
</tbody>
</table>

For example, to create a default AAA authentication method list used with ARAP, use the following command:

```
aaa authentication arap default if-needed none
```

To create the same authentication method list for ARAP and name the list `MIS-access`, use the following command:

```
aaa authentication arap MIS-access if-needed none
```

This section includes the following sections:

**ARAP Authentication Allowing Authorized Guest Logins**

Use the `aaa authentication arap` command with the `auth-guest` keyword to allow guest logins only if the user has already successfully logged in to the EXEC. This method must be the first listed in the ARAP authentication method list but it can be followed by other methods if it does not succeed. For example, to allow all authorized guest logins--meaning logins by users who have already successfully logged in to the EXEC--as the default method of authentication, using RADIUS only if that method fails, enter the following command:
By default, guest logins through ARAP are disabled when you initialize AAA. To allow guest logins, you must use the `aaa authentication arap` command with either the `guest` or the `auth-guest` keyword.

**ARAP Authentication Allowing Guest Logins**

Use the `aaa authentication arap` command with the `guest` keyword to allow guest logins. This method must be the first listed in the ARAP authentication method list but it can be followed by other methods if it does not succeed. For example, to allow all guest logins as the default method of authentication, using RADIUS only if that method fails, enter the following command:

```
aaa authentication arap default guest group radius
```

**ARAP Authentication Using Line Password**

Use the `aaa authentication arap` command with the `method` keyword `line` to specify the line password as the authentication method. For example, to specify the line password as the method of ARAP user authentication when no other method list has been defined, enter the following command:

```
aaa authentication arap default line
```

Before you can use a line password as the ARAP authentication method, you need to define a line password. For more information about defining line passwords, refer to the section Configuring Line Password Protection in this chapter.

**ARAP Authentication Using Local Password**

Use the `aaa authentication arap` command with the `method` keyword `local` to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of ARAP user authentication when no other method list has been defined, enter the following command:

```
aaa authentication arap default local
```

For information about adding users to the local username database, refer to the Establishing Username Authentication.

**ARAP Authentication Using Group RADIUS**

Use the `aaa authentication arap` command with the `group radius` method to specify RADIUS as the ARAP authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication arap default group radius
```

Before you can use RADIUS as the ARAP authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.”
ARAP Authentication Using Group TACACS

Use the `aaa authentication arap` command with the `group tacacs+` method to specify TACACS+ as the ARAP authentication method. For example, to specify TACACS+ as the method of user authentication at login when no other method list has been defined, enter the following command:

```plaintext
aaa authentication arap default group tacacs+
```

Before you can use TACACS+ as the ARAP authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

ARAP Authentication Using Group group-name

Use the `aaa authentication arap` command with the `group group-name` method to specify a subset of RADIUS or TACACS+ servers to use as the ARAP authentication method. To specify and define the group name and the members of the group, use the `aaa group server` command. For example, use the `aaa group server` command to first define the members of `group araprad`:

```plaintext
aaa group server radius araprad
  server 172.16.2.3
  server 172.16.2.17
  server 172.16.2.32
```

This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the group `araprad`.

To specify `group araprad` as the method of user authentication at login when no other method list has been defined, enter the following command:

```plaintext
aaa authentication arap default group araprad
```

Before you can use a group name as the ARAP authentication method, you need to enable communication with the RADIUS or TACACS+ security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.” For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

Configuring NASI Authentication Using AAA

Using the `aaa authentication nasi` command, you can create one or more lists of authentication methods that are tried when NetWare Asynchronous Services Interface (NASI) users attempt to log in to the device. These lists are used with the `nasi authentication line` configuration command.

To configure NASI authentication using AAA, use the following commands starting in global configuration mode:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Device(config)# aaa new-model</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Device(config)# aaa authentication nasi</td>
</tr>
</tbody>
</table>

Example:
## Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Device(config)# line number</th>
<th>(Optional--not needed if default is used in the aaa authentication nasi command) Enters line configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>Device(config-line)# nasi authentication list-name</td>
<td>(Optional--not needed if default is used in the aaa authentication nasi command) Enables authentication for NASI on a line.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Device(config-line)# end</td>
<td>Returns to the privileged EXEC mode.</td>
</tr>
</tbody>
</table>

## What to do next

The `list-name` is any character string used to name the list you are creating. The `method` argument refers to the actual list of methods that the authentication algorithm tries, in the sequence entered.

To create a default list that is used when a named list is not specified in the `aaa authentication nasi` command, use the `default` keyword followed by the methods you want to use in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify `none` as the final method in the command line.

### Note

Because `none` allows all users logging in to be authenticated, it should be used as a backup method of authentication.

The table below lists the supported NASI authentication methods.

### Table 11: AAA Authentication NASI Methods

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>local-case</td>
<td>Uses case-sensitive local username authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>group radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>group tacacs+</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
<tr>
<td>group group-name</td>
<td>Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.</td>
</tr>
</tbody>
</table>
NASI Authentication Using Enable Password

Use the `aaa authentication nasi` command with the keyword `enable` to specify the enable password as the authentication method. For example, to specify the enable password as the method of NASI user authentication when no other method list has been defined, use the following command:

```
aaa authentication nasi default enable
```

Before you can use the enable password as the authentication method, you need to define the enable password. For more information about defining enable passwords, refer to the chapter “Configuring Passwords and Privileges.”

NASI Authentication Using Line Password

Use the `aaa authentication nasi` command with the `method` keyword `line` to specify the line password as the authentication method. For example, to specify the line password as the method of NASI user authentication when no other method list has been defined, enter the following command:

```
aaa authentication nasi default line
```

Before you can use a line password as the NASI authentication method, you need to define a line password. For more information about defining line passwords, refer to the Configuring Line Password Protection.

NASI Authentication Using Local Password

Use the `aaa authentication nasi` command with the `method` keyword `local` to specify that the Cisco router or access server will use the local username database for authentication information. For example, to specify the local username database as the method of NASI user authentication when no other method list has been defined, enter the following command:

```
aaa authentication nasi default local
```

For information about adding users to the local username database, refer to the Establishing Username Authentication.

NASI Authentication Using Group RADIUS

Use the `aaa authentication nasi` command with the `group radius` method to specify RADIUS as the NASI authentication method. For example, to specify RADIUS as the method of NASI user authentication when no other method list has been defined, enter the following command:

```
aaa authentication nasi default group radius
```

Before you can use RADIUS as the NASI authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.”

NASI Authentication Using Group TACACS

Use the `aaa authentication nasi` command with the `group tacacs+` method keyword to specify TACACS+ as the NASI authentication method. For example, to specify TACACS+ as the method of NASI user authentication when no other method list has been defined, enter the following command:

```
aaa authentication nasi default group tacacs+
```
Before you can use TACACS+ as the authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

**NASI Authentication Using group group-name**

Use the `aaa authentication nasi` command with the `group group-name` method to specify a subset of RADIUS or TACACS+ servers to use as the NASI authentication method. To specify and define the group name and the members of the group, use the `aaa group server` command. For example, use the `aaa group server` command to first define the members of `group nasirad`:

```
aaa group server radius nasirad
    server 172.16.2.3
    server 172.16.2.17
    server 172.16.2.32
```

This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the group `nasirad`.

To specify `group nasirad` as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication nasi default group nasirad
```

Before you can use a group name as the NASI authentication method, you need to enable communication with the RADIUS or TACACS+ security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS”. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

**Specifying the Amount of Time for Login Input**

The `timeout login response` command allows you to specify how long the system will wait for login input (such as username and password) before timing out. The default login value is 30 seconds; with the `timeout login response` command, you can specify a timeout value from 1 to 300 seconds. To change the login timeout value from the default of 30 seconds, use the following command in line configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>timeout login response seconds</code></td>
<td>Specifies how long the system will wait for login information before timing out.</td>
</tr>
</tbody>
</table>

**Enabling Password Protection at the Privileged Level**

Use the `aaa authentication enable default` command to create a series of authentication methods that are used to determine whether a user can access the privileged EXEC command level. You can specify up to four authentication methods. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify `none` as the final method in the command line.

Use the following command in global configuration mode:
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `Router(config)# aaa authentication enable default method1 [method2...]` | Enables user ID and password checking for users requesting privileged EXEC level.  
**Note** All `aaa authentication enable default` requests sent by the router to a RADIUS server include the username “$enab15$.” Requests sent to a TACACS+ server will include the username that is entered for login authentication. |

The method argument refers to the actual list of methods the authentication algorithm tries, in the sequence entered. the table below lists the supported enable authentication methods.

### Table 12: AAA Authentication Enable Default Methods

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td><code>line</code></td>
<td>Uses the line password for authentication.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td><code>group radius</code></td>
<td>Uses the list of all RADIUS hosts for authentication.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The RADIUS method does not work on a per-username basis.</td>
</tr>
<tr>
<td><code>group tacacs+</code></td>
<td>Uses the list of all TACACS+ hosts for authentication.</td>
</tr>
<tr>
<td><code>group</code> <code>group-name</code></td>
<td>Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <code>aaa group server radius</code> or <code>aaa group server tacacs+</code> command.</td>
</tr>
</tbody>
</table>

### Changing the Text Displayed at the Password Prompt

Use the `aaa authentication password-prompt` command to change the default text that the Cisco IOS XE software displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The `no` form of this command returns the password prompt to the following default value:

**Password:**

The `aaa authentication password-prompt` command does not change any dialog that is supplied by a remote TACACS+ or RADIUS server.

The `aaa authentication password-prompt` command works when RADIUS is used as the login method. You will be able to see the password prompt defined in the command shown even when the RADIUS server is unreachable. The `aaa authentication password-prompt` command does not work with TACACS+. TACACS+ supplies the NAS with the password prompt to display to the users. If the TACACS+ server is reachable, the NAS gets the password prompt from the server and uses that prompt instead of the one defined in the `aaa authentication password-prompt` command. If the TACACS+ server is not reachable, the password prompt defined in the `aaa authentication password-prompt` command may be used.

Use the following command in global configuration mode:
Purpose

Command

- **Router(config)# aaa authentication password-prompt text-string**

Purpose:
Changes the default text displayed when a user is prompted to enter a password.

### Preventing an Access Request with a Blank Username from Being Sent to the RADIUS Server

The following configuration steps provide the ability to prevent an Access Request with a blank username from being sent to the RADIUS server. This functionality ensures that unnecessary RADIUS server interaction is avoided, and RADIUS logs are kept short.

**Note**

The **aaa authentication suppress null-username** command is available beginning in Cisco IOS XE Release 2.4.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
  enable  
  Example:
  Device> enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Step 2**  
  configure terminal  
  Example:
  Device# configure terminal | Enters global configuration mode. |
| **Step 3**  
  aaa new-model  
  Example:
  Device(config)# configure terminal | Enables AAA globally. |
| **Step 4**  
  aaa authentication suppress null-username  
  Example:
  Device(config)# aaa authentication suppress null-username | Prevents an Access Request with a blank username from being sent to the RADIUS server. |

### Configuring Message Banners for AAA Authentication

AAA supports the use of configurable, personalized login and failed-login banners. You can configure message banners that will be displayed when a user logs in to the system to be authenticated using AAA and when, for whatever reason, authentication fails.
Configuring a Login Banner

To configure a banner that is displayed when a user logs in (replacing the default message for login), perform the following task:

Before you begin

To create a login banner, you must configure a delimiting character that notifies the system that the following text string must be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string for the banner.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>aaa new-model</code></td>
<td>Enables AAA.</td>
</tr>
<tr>
<td><code>Device(config)# aaaa new-model</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | |
| `Device(config)# aaa authentication banner delimiter string delimiter` | Creates a personalized login banner. |

| **Step 3** | |
| `Device(config)# end` | Returns to privileged EXEC mode. |

What to do next

After you have configured a login banner, you must complete basic authentication configuration using AAA if you have not already done so. For information about the different types of AAA authentication available, please refer to “Configuring Authentication” in the *Authentication, Authorization, and Accounting Configuration Guide*.

Configuring a Failed-Login Banner

To configure a message that is displayed when a user login fails (replacing the default message for failed login), perform the following task:

Before you begin

To create a failed-login banner, you must configure a delimiting character, which notifies the system that the following text string must be displayed as the banner, and then configure the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the failed-login banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# aaa new-model</code></td>
<td>Enables AAA.</td>
</tr>
</tbody>
</table>

| **Step 2** | |
| `Device(config)# aaa authentication fail-message delimiter string delimiter` | Creates a message to be displayed when a user login fails. |
### What to do next

After you have configured a failed-login banner, you must complete basic authentication configuration using AAA if you have not already done so. For information about the different types of AAA authentication available, please refer to “Configuring Authentication” in the *Authentication, Authorization, and Accounting Configuration Guide*.

### Configuring AAA Packet of Disconnect

Packet of disconnect (POD) terminates connections on the network access server (NAS) when particular session attributes are identified. By using session information obtained from AAA, the POD client residing on a UNIX workstation sends disconnect packets to the POD server running on the network access server. The NAS terminates any inbound user session with one or more matching key attributes. It rejects requests when required fields are missing or when an exact match is not found.

To configure POD, perform the following tasks in global configuration mode:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Device(config)# aaa accounting network default</td>
<td>Enables AAA accounting records.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>start-stop radius</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Device(config)# aaa accounting delay-start</td>
<td>(Optional) Delays generation of the start accounting record until the Framed-IP-Address is assigned, allowing its use in the POD packet.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Device(config)# aaa pod server server-keystring</td>
<td>Enables POD reception.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Device(config)# radius-server host IP address non-standard</td>
<td>Declares a RADIUS host that uses a vendor-proprietary version of RADIUS.</td>
</tr>
</tbody>
</table>

### Enabling Double Authentication

Depending on the Cisco release, PPP sessions could be authenticated only by using a single authentication method: either PAP or CHAP. Double authentication requires remote users to pass a second stage of authentication (after CHAP or PAP authentication) before gaining network access.

This second (“double”) authentication requires a password that is known to the user but not stored on the user’s remote host. Therefore, the second authentication is specific to a user, not to a host. This provides an
additional level of security that will be effective even if information from the remote host is stolen. In addition, this also provides greater flexibility by allowing customized network privileges for each user.

The second stage authentication can use one-time passwords such as token card passwords, which are not supported by CHAP. If one-time passwords are used, a stolen user password is of no use to the perpetrator.

**How Double Authentication Works**

With double authentication, there are two authentication/authorization stages. These two stages occur after a remote user dials in and a PPP session is initiated.

In the first stage, the user logs in using the remote host name; CHAP (or PAP) authenticates the remote host, and then PPP negotiates with AAA to authorize the remote host. In this process, the network access privileges associated with the remote host are assigned to the user.

We suggest that the network administrator restrict authorization at this first stage to allow only Telnet connections to the local host.

In the second stage, the remote user must Telnet to the network access server to be authenticated. When the remote user logs in, the user must be authenticated with AAA login authentication. The user then must enter the `access-profile` command to be reauthorized using AAA. When this authorization is complete, the user has been double authenticated, and can access the network according to per-user network privileges.

The system administrator determines what network privileges remote users will have after each stage of authentication by configuring appropriate parameters on a security server. To use double authentication, the user must activate it by issuing the `access-profile` command.

Double authentication can cause certain undesirable events if multiple hosts share a PPP connection to a network access server, as shown in the figure below. First, if a user, Bob, initiates a PPP session and activates double authentication at the network access server (per the figure below), any other user will automatically have the same network privileges as Bob until Bob’s PPP session expires. This happens because Bob’s authorization profile is applied to the network access server’s interface during the PPP session and any PPP traffic from other users will use the PPP session Bob established. Second, if Bob initiates a PPP session and activates double authentication, and then--before Bob’s PPP session has expired--another user, Jane, executes the `access-profile` command (or, if Jane Telnets to the network access server and `autocommand access-profile` is executed), a reauthorization will occur and Jane’s authorization profile will be applied to the interface--replacing Bob’s profile. This can disrupt or halt Bob’s PPP traffic, or grant Bob additional authorization privileges Bob should not have.

**Figure 2: Possibly Risky Topology: Multiple Hosts Share a PPP Connection to a Network Access Server**

[Diagram showing network topology with Bob, Jane, Remote host, Local host, AAA server, and PPP connections]
Configuring Double Authentication

To configure double authentication, you must complete the following steps:

1. Enable AAA by using the `aaa-new-model` global configuration command. For more information about enabling AAA, refer to the chapter “AAA Overview.”

2. Use the `aaa authentication` command to configure your network access server to use login and PPP authentication method lists, then apply those method lists to the appropriate lines or interfaces.

3. Use the `aaa authorization` command to configure AAA network authorization at login. For more information about configuring network authorization, refer to the “Configuring Authorization” chapter.

4. Configure security protocol parameters (for example, RADIUS or TACACS+). For more information about RADIUS, refer to the chapter “Configuring RADIUS”. For more information about TACACS+, refer to the chapter “Configuring TACACS+.”

5. Use access control list AV pairs on the security server that the user can connect to the local host only by establishing a Telnet connection.

6. (Optional) Configure the `access-profile` command as an autocommand. If you configure the autocommand, remote users will not have to manually enter the `access-profile` command to access authorized rights associated with their personal user profile.

---

**Note**

If the `access-profile` command is configured as an autocommand, users will still have to Telnet to the local host and log in to complete double authentication.

Follow these rules when creating the user-specific authorization statements (These rules relate to the default behavior of the `access-profile` command):

- Use valid AV pairs when configuring access control list AV pairs on the security server.

- If you want remote users to use the interface’s existing authorization (that which existed prior to the second stage authentication/authorization), but you want them to have different access control lists (ACLs), you should specify only ACL AV pairs in the user-specific authorization definition. This might be desirable if you set up a default authorization profile to apply to the remote host, but want to apply specific ACLs to specific users.

- When these user-specific authorization statements are later applied to the interface, they can either be added to the existing interface configuration or they can replace the existing interface configuration—depending on which form of the `access-profile` command is used to authorize the user. You should understand how the `access-profile` command works before configuring the authorization statements.

- If you will be using ISDN or Multilink PPP, you must also configure virtual templates at the local host.

To troubleshoot double authentication, use the `debug aaa per-user` debug command. For more information about this command, refer to the *Cisco IOS Debug Command Reference*.

**Accessing the User Profile After Double Authentication**

In double authentication, when a remote user establishes a PPP link to the local host using the local host name, the remote host is CHAP (or PAP) authenticated. After CHAP (or PAP) authentication, PPP negotiates with
AAA to assign network access privileges associated with the remote host to the user. (We suggest that privileges at this stage be restricted to allow the user to connect to the local host only by establishing a Telnet connection.)

When the user needs to initiate the second phase of double authentication, establishing a Telnet connection to the local host, the user enters a personal username and password (different from the CHAP or PAP username and password). This action causes AAA reauthentication to occur according to the personal username/password. The initial rights associated with the local host, though, are still in place. By using the access-profile command, the rights associated with the local host are replaced by or merged with those defined for the user in the user’s profile.

To access the user profile after double authentication, use the following command in EXEC configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router&gt; access-profile [merge</td>
<td>replace] ignore-sanity-checks</td>
</tr>
</tbody>
</table>

If you configured the access-profile command to be executed as an autocommand, it will be executed automatically after the remote user logs in.

### Enabling Automated Double Authentication

You can make the double authentication process easier for users by implementing automated double authentication. Automated double authentication provides all of the security benefits of double authentication, but offers a simpler, more user-friendly interface for remote users. With double authentication, a second level of user authentication is achieved when the user Telnets to the network access server or router and enters a username and password. With automated double authentication, the user does not have to Telnet to the network access server; instead the user responds to a dialog box that requests a username and password or personal identification number (PIN). To use the automated double authentication feature, the remote user hosts must be running a companion client application.

**Note**

Automated double authentication, like the existing double authentication feature, is for Multilink PPP ISDN connections only. Automated double authentication cannot be used with other protocols such as X.25 or SLIP.

Automated double authentication is an enhancement to the existing double authentication feature. To configure automated double authentication, you must first configure double authentication by completing the following steps:

1. Enable AAA by using the **aaa-new model** global configuration command.

2. Use the **aaa authentication** command to configure your network access server to use login and PPP authentication method lists, then apply those method lists to the appropriate lines or interfaces.

3. Use the **aaa authorization** command to configure AAA network authorization at login. For more information about configuring network authorization, refer to the chapter “Configuring Authorization.”

4. Configure security protocol parameters (for example, RADIUS or TACACS+). For more information about RADIUS, refer to the chapter “Configuring RADIUS”. For more information about TACACS+, refer to the chapter “Configuring TACACS+.”
5. Use access control list AV pairs on the security server that the user can connect to the local host only by establishing a Telnet connection.

6. Configure the access-profile command as an autocmd. If you configure the autocmd, remote users will not have to manually enter the access-profile command to access authorized rights associated with their personal user profile. To learn about configuring autocmds, refer to the autocmd command in the CiscoIOS Dial Technologies Command Reference, Release 12.2.

---

**Note**

If the access-profile command is configured as an autocmd, users will still have to Telnet to the local host and log in to complete double authentication.

Follow these rules when creating the user-specific authorization statements (These rules relate to the default behavior of the access-profile command):

- Use valid AV pairs when configuring access control list AV pairs on the security server.

- If you want remote users to use the interface’s existing authorization (that which existed prior to the second stage authentication/authorization), but you want them to have different access control lists (ACLS), you should specify only ACL AV pairs in the user-specific authorization definition. This might be desirable if you set up a default authorization profile to apply to the remote host, but want to apply specific ACLs to specific users.

- When these user-specific authorization statements are later applied to the interface, they can either be added to the existing interface configuration, or replace the existing interface configuration--depending on which form of the access-profile command is used to authorize the user. You should understand how the access-profile command works before configuring the authorization statements.

- If you will be using ISDN or Multilink PPP, you must also configure virtual templates at the local host.

To troubleshoot double authentication, use the debug aaa per-user debug command. For more information about this command, refer to the Cisco IOS Debug Command Reference.

After you have configured double authentication, you are ready to configure the automation enhancement.

### Configuring Automated Double Authentication

To configure automated double authentication, use the following commands, starting in global configuration mode.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Device(config)# ip trigger-authentication</td>
<td>Enables automation of double authentication.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>[timeout seconds] [port number]</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> Do one of the following:</td>
<td>Selects an ISDN BRI or ISDN PRI interface and enter the interface configuration mode.</td>
</tr>
<tr>
<td>• Device(config)# interface bri number</td>
<td></td>
</tr>
</tbody>
</table>
### Troubleshooting Automated Double Authentication

To troubleshoot automated double authentication, use the following commands in privileged EXEC mode:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Device# show ip trigger-authentication</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Device# clear ip trigger-authentication</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Device# debug ip trigger-authentication</td>
</tr>
</tbody>
</table>

---

### Configuring the Dynamic Authorization Service for RADIUS CoA

Use the following procedure to enable the router as an authentication, authorization, and accounting (AAA) server for dynamic authorization service to support the CoA functionality that pushes the policy map in an input and output direction.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable  
Example:  
Router> enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Step 2** | configure terminal  
Example:  
Router# configure terminal | Enters global configuration mode. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>aaa new-model</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config)# aaa new-model</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>aaa server radius dynamic-author</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config)# aaa server radius dynamic-author</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>**client ip_addr</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>**domain delimiter character</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>port port-num</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config-locsvr-da-radius)# port 3799</td>
</tr>
</tbody>
</table>

**Configuring a Device to Ignore Bounce and Disable RADIUS CoA Requests**

When an authentication port is authenticated with multiple hosts and there is a Change of Authorization (CoA) request for one host to flap on this port or one host session to be terminated on this port, the other hosts on
this port are also affected. Thus, an authenticated port with multiple hosts can trigger a DHCP renegotiation from one or more hosts in the case of a flap, or it can administratively shut down the authentication port that is hosting the session for one or more hosts.

Perform the following steps to configure the device to ignore RADIUS server Change of Authorization (CoA) requests in the form of a bounce port command or disable port command.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
|        | Example:
|        | Device> enable                                | • Enter your password if prompted.                                      |
| Step 2 | configure terminal                            | Enters global configuration mode.                                       |
|        | Example:
|        | Device# configure terminal                    |                                                                         |
| Step 3 | aaa new-model                                 | Enables authentication, authorization, and accounting (AAA) globally.    |
|        | Example:
|        | Device(config)# aaa new-model                 |                                                                         |
| Step 4 | authentication command bounce-port ignore     | (Optional) Configures the device to ignore a RADIUS server bounce port command that causes a host to link flap on an authentication port, which causes DHCP renegotiation from one or more hosts connected to this port. |
|        | Example:
|        | Device(config)# authentication command bounce-port ignore |                                                                         |
| Step 5 | authentication command disable-port ignore    | (Optional) Configures the device to ignore a RADIUS server CoA disable port command that administratively shuts down the authentication port that hosts one or more host sessions. |
|        | Example:
|        | Device(config)# authentication command disable-port ignore | • The shutting down of the port causes session termination.             |
| Step 6 | end                                           | Returns to privileged EXEC mode.                                        |
|        | Example:
|        | Device(config)# end                           |                                                                         |
## Configuring Domain Stripping at the Server Group Level

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>aaa group server radius server-name</code></td>
<td>Adds the RADIUS server and enters server group RADIUS configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>• The <code>server-name</code> argument specifies the RADIUS server group name.</td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# aaa group server radius radi</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>domain-stripping [strip-suffix word] [right-to-left ] [prefix-delimiter word] [delimiter word]</code></td>
<td>Configures domain stripping at the server group level.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-sg-radius)# domain-stripping delimiter username@example.com</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>end</code></td>
<td>Exits server group RADIUS configuration mode and returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-sg-radius)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

## Non-AAA Authentication Methods

### Configuring Line Password Protection

You can This task is used to provide access control on a terminal line by entering the password and establishing password checking.

**Note**

If you configure line password protection and then configure TACACS or extended TACACS, the TACACS username and password take precedence over line passwords. If you have not yet implemented a security policy, we recommend that you use AAA.
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Enters your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>**line [aux</td>
<td>console</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# line console 0</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>password password</strong></td>
<td>Assigns a password to a terminal or other device on a line. The password checker is case sensitive and can include spaces; for example, the password “Secret” is different from the password “secret,” and “two words” is an acceptable password.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-line)# secret word</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>login</strong></td>
<td>Enables password checking at login.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-line)# login</td>
<td>You can disable line password verification by disabling password checking by using the <strong>no</strong> version of this command.</td>
</tr>
</tbody>
</table>

**Note** The **login** command only changes username and privilege level but it does not execute a shell; therefore autocommands will not be executed. To execute autocommands under this circumstance, you need to establish a Telnet session back into the router (loop-back). Make sure that the router has been configured for secure Telnet sessions if you choose to implement autocommands this way.

### Establishing Username Authentication

You can create a username-based authentication system, which is useful in the following situations:

- To provide a TACACS-like username and encrypted password-authentication system for networks that cannot support TACACS
To provide special-case logins: for example, access list verification, no password verification, autocommand execution at login, and “no escape” situations

To establish username authentication, use the following commands in global configuration mode as needed for your system configuration:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Do one of the following:</td>
<td>Establishes username authentication with encrypted passwords.</td>
</tr>
<tr>
<td></td>
<td>• Device(config)# <strong>username</strong> name</td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>[nopassword</td>
<td>password password</td>
</tr>
<tr>
<td></td>
<td>• Device(config)# <strong>username</strong> name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[access-class number]</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Device(config)# <strong>username</strong> name [<strong>privilege level</strong>]</td>
<td>(Optional) Sets the privilege level for the user.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Device(config)# <strong>username</strong> name [<strong>autocommand command</strong>]</td>
<td>(Optional) Specifies a command to be executed automatically.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Device(config)# <strong>username</strong> name [<strong>noescape</strong>] [<strong>nohangup</strong>]</td>
<td>(Optional) Sets a “no escape” login environment.</td>
</tr>
</tbody>
</table>

### What to do next

The keyword **noescape** prevents users from using escape characters on the hosts to which they are connected. The **nohangup** feature does not disconnect after using the autocommand.

---

Password encryption is enabled by default. To change the password encryption:

Caution

Passwords will be displayed in clear text in your configuration unless you enable the **service password-encryption** command. For more information about the **service password-encryption** command, refer to the Cisco IOS Security Command Reference.

---

### Enabling CHAP or PAP Authentication

One of the most common transport protocols used in Internet service providers’ (ISPs’) dial solutions is the Point-to-Point Protocol (PPP). Traditionally, remote users dial in to an access server to initiate a PPP session. After PPP has been negotiated, remote users are connected to the ISP network and to the Internet.

Because ISPs want only customers to connect to their access servers, remote users are required to authenticate to the access server before they can start up a PPP session. Normally, a remote user authenticates by typing in a username and password when prompted by the access server. Although this is a workable solution, it is difficult to administer and awkward for the remote user.
A better solution is to use the authentication protocols built into PPP. In this case, the remote user dials in to the access server and starts up a minimal subset of PPP with the access server. This does not give the remote user access to the ISP’s network—it merely allows the access server to talk to the remote device.

PPP currently supports two authentication protocols: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Both are specified in RFC 1334 and are supported on synchronous and asynchronous interfaces. Authentication via PAP or CHAP is equivalent to typing in a username and password when prompted by the server. CHAP is considered to be more secure because the remote user’s password is never sent across the connection.

PPP (with or without PAP or CHAP authentication) is also supported in dialout solutions. An access server utilizes a dialout feature when it initiates a call to a remote device and attempts to start up a transport protocol such as PPP.

See the *Cisco IOS XE Dial Technologies Configuration Guide*, Release 2 for more information about CHAP and PAP.

---

**Note**

To use CHAP or PAP, you must be running PPP encapsulation.

When CHAP is enabled on an interface and a remote device attempts to connect to it, the access server sends a CHAP packet to the remote device. The CHAP packet requests or “challenges” the remote device to respond. The challenge packet consists of an ID, a random number, and the host name of the local router.

When the remote device receives the challenge packet, it concatenates the ID, the remote device’s password, and the random number, and then encrypts all of it using the remote device’s password. The remote device sends the results back to the access server, along with the name associated with the password used in the encryption process.

When the access server receives the response, it uses the name it received to retrieve a password stored in its user database. The retrieved password should be the same password the remote device used in its encryption process. The access server then encrypts the concatenated information with the newly retrieved password--if the result matches the result sent in the response packet, authentication succeeds.

The benefit of using CHAP authentication is that the remote device’s password is never transmitted in clear text. This prevents other devices from stealing it and gaining illegal access to the ISP’s network.

CHAP transactions occur only at the time a link is established. The access server does not request a password during the rest of the call. (The local device can, however, respond to such requests from other devices during a call.)

When PAP is enabled, the remote router attempting to connect to the access server is required to send an authentication request. If the username and password specified in the authentication request are accepted, the Cisco IOS XE software sends an authentication acknowledgment.

After you have enabled CHAP or PAP, the access server will require authentication from remote devices dialing in to the access server. If the remote device does not support the enabled protocol, the call will be dropped.

To use CHAP or PAP, you must perform the following tasks:

1. Enable PPP encapsulation.
2. Enable CHAP or PAP on the interface.
3. For CHAP, configure host name authentication and the secret or password for each remote system with which authentication is required.
Enabling PPP Encapsulation

To enable PPP encapsulation, use the following command in interface configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-if)# encapsulation ppp</td>
<td>Enables PPP on an interface.</td>
</tr>
</tbody>
</table>

Enabling PAP or CHAP

To enable CHAP or PAP authentication on an interface configured for PPP encapsulation, use the following command in interface configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-if)# ppp authentication {protocol1 [protocol2...]</td>
<td>Defines the authentication protocols supported and the order in which they are used. In this command, protocol1, protocol2 represent the following protocols: CHAP, MS-CHAP, and PAP. PPP authentication is attempted first using the first authentication method, which is protocol1. If protocol1 is unable to establish authentication, the next configured protocol is used to negotiate authentication.</td>
</tr>
</tbody>
</table>

If you configure `ppp authentication chap` on an interface, all incoming calls on that interface that initiate a PPP connection will have to be authenticated using CHAP; likewise, if you configure `ppp authentication pap`, all incoming calls that start a PPP connection will have to be authenticated via PAP. If you configure `ppp authentication chap pap`, the access server will attempt to authenticate all incoming calls that start a PPP session with CHAP. If the remote device does not support CHAP, the access server will try to authenticate the call using PAP. If the remote device does not support either CHAP or PAP, authentication will fail and the call will be dropped. If you configure `ppp authentication pap chap`, the access server will attempt to authenticate all incoming calls that start a PPP session with PAP. If the remote device does not support PAP, the access server will try to authenticate the call using CHAP. If the remote device does not support either protocol, authentication will fail and the call will be dropped. If you configure the `ppp authentication` command with the `callin` keyword, the access server will only authenticate the remote device if the remote device initiated the call.

Authentication method lists and the `one-time` keyword are only available if you have enabled AAA--they will not be available if you are using TACACS or extended TACACS. If you specify the name of an authentication method list with the `ppp authentication` command, PPP will attempt to authenticate the connection using the methods defined in the specified method list. If AAA is enabled and no method list is defined by name, PPP will attempt to authenticate the connection using the methods defined as the default. The `ppp authentication` command with the `one-time` keyword enables support for one-time passwords during authentication.

The `if-needed` keyword is only available if you are using TACACS or extended TACACS. The `ppp authentication` command with the `if-needed` keyword means that PPP will only authenticate the remote device via PAP or CHAP if they have not yet authenticated during the life of the current call. If the remote device authenticated via a standard login procedure and initiated PPP from the EXEC prompt, PPP will not authenticate via CHAP if `ppp authentication chap if-needed` is configured on the interface.

⚠️ Caution

If you use a `list-name` that has not been configured with the `aaa authentication ppp` command, you disable PPP on the line.
Inbound and Outbound Authentication

PPP supports two-way authentication. Normally, when a remote device dials in to an access server, the access server requests that the remote device prove that it is allowed access. This is known as inbound authentication. At the same time, the remote device can also request that the access server prove that it is who it says it is. This is known as outbound authentication. An access server also does outbound authentication when it initiates a call to a remote device.

Enabling Outbound PAP Authentication

To enable outbound PAP authentication, use the following command in interface configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-if)# ppp pap sent-username username password password</td>
<td>Enables outbound PAP authentication.</td>
</tr>
</tbody>
</table>

The access server uses the username and password specified by the `ppp pap sent-username` command to authenticate itself whenever it initiates a call to a remote device or when it has to respond to a remote device’s request for outbound authentication.

Refusing PAP Authentication Requests

To refuse PAP authentication from peers requesting it, meaning that PAP authentication is disabled for all calls, use the following command in interface configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-if)# ppp pap refuse</td>
<td>Refuses PAP authentication from peers requesting PAP authentication.</td>
</tr>
</tbody>
</table>

If the refuse keyword is not used, the router will not refuse any PAP authentication challenges received from the peer.

Creating a Common CHAP Password

For remote CHAP authentication only, you can configure your router to create a common CHAP secret password to use in response to challenges from an unknown peer; for example, if your router calls a rotary of routers (either from another vendor, or running an older version of the Cisco IOS software) to which a new (that is, unknown) router has been added. The `ppp chap password` command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

To enable a router calling a collection of routers to configure a common CHAP secret password, use the following command in interface configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-if)# ppp chap password secret</td>
<td>Enables a router calling a collection of routers to configure a common CHAP secret password.</td>
</tr>
</tbody>
</table>
Refusing CHAP Authentication Requests

To refuse CHAP authentication from peers requesting it, meaning that CHAP authentication is disabled for all calls, use the following command in interface configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config-if)# ppp chap refuse [callin]</code></td>
<td>Refuses CHAP authentication from peers requesting CHAP authentication.</td>
</tr>
</tbody>
</table>

If the `callin` keyword is used, the router will refuse to answer CHAP authentication challenges received from the peer, but will still require the peer to answer any CHAP challenges the router sends.

If outbound PAP has been enabled (using the `ppp pap sent-username` command), PAP will be suggested as the authentication method in the refusal packet.

Delaying CHAP Authentication Until Peer Authenticates

To specify that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router, use the following command in interface configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config-if)# ppp chap wait secret</code></td>
<td>Configures the router to delay CHAP authentication until after the peer has authenticated itself to the router.</td>
</tr>
</tbody>
</table>

This command (which is the default) specifies that the router will not authenticate to a peer requesting CHAP authentication until the peer has authenticated itself to the router. The `no ppp chap wait` command specifies that the router will respond immediately to an authentication challenge.

Using MS-CHAP

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is the Microsoft version of CHAP and is an extension of RFC 1994. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; in this case, authentication occurs between a PC using Microsoft Windows NT or Microsoft Windows 95 and a Cisco device or access server acting as a network access server.

MS-CHAP differs from the standard CHAP as follows:

- MS-CHAP is enabled by negotiating CHAP Algorithm 0x80 in LCP option 3, Authentication Protocol.
- The MS-CHAP Response packet is in a format designed to be compatible with Microsoft Windows NT 3.5 and 3.51, Microsoft Windows 95, and Microsoft LAN Manager 2.x. This format does not require the authenticator to store a clear or reversibly encrypted password.
- MS-CHAP provides an authenticator-controlled authentication retry mechanism.
- MS-CHAP provides an authenticator-controlled change password mechanism.
- MS-CHAP defines a set of “reason-for-failure” codes returned in the Failure packet message field.

Depending on the security protocols you have implemented, PPP authentication using MS-CHAP can be used with or without AAA security services. If you have enabled AAA, PPP authentication using MS-CHAP can
Defining PPP Authentication using MS-CHAP

To define PPP authentication using MS-CHAP, use the following commands in interface configuration mode:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Device(config-if)# encapsulation ppp</td>
<td>Enables PPP encapsulation.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Device(config-if)# ppp authentication ms-chap [if-needed] [list-name</td>
<td>default] [callin] [one-time]</td>
</tr>
</tbody>
</table>

**What to do next**

If you configure `ppp authentication ms-chap` on an interface, all incoming calls on that interface that initiate a PPP connection will have to be authenticated using MS-CHAP. If you configure the `ppp authentication` command with the `callin` keyword, the access server will only authenticate the remote device if the remote device initiated the call.

Authentication method lists and the `one-time` keyword are only available if you have enabled AAA--they will not be available if you are using TACACS or extended TACACS. If you specify the name of an authentication method list with the `ppp authentication` command, PPP will attempt to authenticate the connection using the methods defined in the specified method list. If AAA is enabled and no method list is defined by name, PPP will attempt to authenticate the connection using the methods defined as the default. The `ppp authentication` command with the `one-time` keyword enables support for one-time passwords during authentication.

The `if-needed` keyword is only available if you are using TACACS or extended TACACS. The `ppp authentication` command with the `if-needed` keyword means that PPP will only authenticate the remote device via MS-CHAP if that device has not yet authenticated during the life of the current call. If the remote device authenticated through a standard login procedure and initiated PPP from the EXEC prompt, PPP will not authenticate through MS-CHAP if `ppp authentication chap if-needed` is configured.

---

be used in conjunction with both TACACS+ and RADIUS. The table below lists the vendor-specific RADIUS attributes (IETF Attribute 26) that enable RADIUS to support MS-CHAP.

**Table 13: Vendor-Specific RADIUS Attributes for MS-CHAP**

<table>
<thead>
<tr>
<th>Vendor-ID Number</th>
<th>Vendor-Type Number</th>
<th>Vendor-Proprietary Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>311</td>
<td>11</td>
<td>MSCHAP-Challenge</td>
<td>Contains the challenge sent by a network access server to an MS-CHAP user. It can be used in both Access-Request and Access-Challenge packets.</td>
</tr>
<tr>
<td>211</td>
<td>11</td>
<td>MSCHAP-Response</td>
<td>Contains the response value provided by a PPP MS-CHAP user in response to the challenge. It is only used in Access-Request packets. This attribute is identical to the PPP CHAP Identifier.</td>
</tr>
</tbody>
</table>
If PPP authentication using MS-CHAP is used with username authentication, you must include the MS-CHAP secret in the local username/password database. For more information about username authentication, refer to the “Establish Username Authentication” section.

### Authentication Examples

#### Example: RADIUS Authentication

This section provides two sample configurations using RADIUS.

The following example shows how to configure the router to authenticate and authorize using RADIUS:

```config
aaa authentication login radius-login group radius local
aaa authentication ppp radius-ppp if-needed group radius
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
line 3
  login authentication radius-login
interface serial 0
  ppp authentication radius-ppp
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

- The `aaa authentication login radius-login group radius local` command configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database.

- The `aaa authentication ppp radius-ppp if-needed group radius` command configures the Cisco IOS XE software to use PPP authentication using CHAP or PAP if the user has not already logged in. If the EXEC facility has authenticated the user, PPP authentication is not performed.

- The `aaa authorization exec default group radius if-authenticated` command queries the RADIUS database for information that is used during EXEC authorization, such as autocommands and privilege levels, but only provides authorization if the user has successfully authenticated.

- The `aaa authorization network default group radius` command queries RADIUS for network authorization, address assignment, and other access lists.

- The `login authentication radius-login` command enables the radius-login method list for line 3.

- The `ppp authentication radius-ppp` command enables the radius-ppp method list for serial interface 0.

The following example shows how to configure the router to prompt for and verify a username and password, authorize the user’s EXEC level, and specify it as the method of authorization for privilege level 2. In this example, if a local username is entered at the username prompt, that username is used for authentication.

If the user is authenticated using the local database, EXEC authorization using RADIUS will fail because no data is saved from the RADIUS authentication. The method list also uses the local database to find an autocommand. If there is no autocommand, the user becomes the EXEC user. If the user then attempts to issue commands that are set at privilege level 2, TACACS+ is used to attempt to authorize the command.

```config
aaa authentication login default group radius local
aaa authorization exec default group radius local
```
aaa authorization command 2 default group tacacs+ if-authenticated
radius-server host 172.16.71.146 auth-port 1645 acct-port 1646
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

- The `aaa authorization login default group radius local` command specifies that the username and password are verified by RADIUS or, if RADIUS is not responding, by the router’s local user database.

- The `aaa authorization exec default group radius local` command specifies that RADIUS authentication information be used to set the user’s EXEC level if the user authenticates with RADIUS. If no RADIUS information is used, this command specifies that the local user database be used for EXEC authorization.

- The `aaa authorization command 2 default group tacacs+ if-authenticated` command specifies TACACS+ authorization for commands set at privilege level 2, if the user has already successfully authenticated.

- The `radius-server host 172.16.71.146 auth-port 1645 acct-port 1646` command specifies the IP address of the RADIUS server host, the UDP destination port for authentication requests, and the UDP destination port for accounting requests.

- The `radius-server attribute 44 include-in-access-req` command sends RADIUS attribute 44 (Acct-Session-ID) in access-request packets.

- The `radius-server attribute 8 include-in-access-req` command sends RADIUS attribute 8 (Framed-IP-Address) in access-request packets.

Example: TACACS Authentication

The following example shows how to configure TACACS+ as the security protocol to be used for PPP authentication:

```
aaa new-model
aaa authentication ppp test group tacacs+ local
interface serial 0
ppp authentication chap pap test
tacacs-server host 192.0.2.3
tacacs-server key goaway
```

The lines in this sample TACACS+ authentication configuration are defined as follows:

- The `aaa new-model` command enables the AAA security services.

- The `aaa authentication ppp test group tacacs+ local` command defines a method list, “test,” to be used on serial interfaces running PPP. The keywords `group tacacs+` means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword `local` indicates that authentication will be attempted using the local database on the network access server.

- The `interface serial 0` command selects the line.

- The `ppp authentication chap pap test` command applies the test method list to this line.

- The `tacacs-server host` command identifies the TACACS+ daemon as having an IP address of 192.0.2.3.

- The `tacacs-server key` command defines the shared encryption key to be “goaway.”

The following example shows how to configure AAA authentication for PPP:
aaa authentication ppp default if-needed group tacacs+ local

In this example, the keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP is not necessary and can be skipped. If authentication is needed, the keywords **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

The following example shows how to create the same authentication algorithm for PAP, but it calls the method list “MIS-access” instead of “default”:

aaa authentication ppp MIS-access if-needed group tacacs+ local
interface serial 0
ppp authentication pap MIS-access

In this example, because the list does not apply to any interfaces (unlike the default list, which applies automatically to all interfaces), the administrator must select interfaces to which this authentication scheme should apply by using the **interface** command. The administrator must then apply this method list to those interfaces by using the **ppp authentication** command.

**Example: Kerberos Authentication**

To specify Kerberos as the login authentication method, use the following command:

aaa authentication login default krb5

To specify Kerberos authentication for PPP, use the following command:

aaa authentication ppp default krb5

**Example: AAA Scalability**

The following example shows a general security configuration using AAA with RADIUS as the security protocol. In this example, the network access server is configured to allocate 16 background processes to handle AAA requests for PPP.

aaa new-model
radius-server host alcatraz
radius-server key myRADIUSpassWoRd
radius-server configure-nas
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authentication login admins local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa processes 16
line 1 16
   autoselect ppp
   autoselect during-login
   login authentication admins
   modem dialin
interface group-async 1
   group-range 1 16
   encapsulation ppp
   ppp authentication pap dialins
The lines in this sample RADIUS AAA configuration are defined as follows:

- The `aaa new-model` command enables AAA network security services.
- The `radius-server host` command defines the name of the RADIUS server host.
- The `radius-server key` command defines the shared secret text string between the network access server and the RADIUS server host.
- The `radius-server configure-nas` command defines that the Cisco router or access server will query the RADIUS server for static routes and IP pool definitions when the device first starts up.
- The `username` command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.
- The `aaa authentication ppp dialins group radius local` command defines the authentication method list “dialins,” which specifies that RADIUS authentication, then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The `aaa authentication login admins local` command defines another method list, “admins,” for login authentication.
- The `aaa authorization network default group radius local` command is used to assign an address and other network parameters to the RADIUS user.
- The `aaa accounting network default start-stop group radius` command tracks PPP usage.
- The `aaa processes` command allocates 16 background processes to handle AAA requests for PPP.
- The `line` command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.
- The `autoselect ppp` command allows a PPP session to start up automatically on these selected lines.
- The `autoselect during-login` command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.
- The `login authentication admins` command applies the “admins” method list for login authentication.
- The `modem dialin` command configures modems attached to the selected lines to only accept incoming calls.
- The `interface group-async` command selects and defines an asynchronous interface group.
- The `group-range` command defines the member asynchronous interfaces in the interface group.
- The `encapsulation ppp` command sets PPP as the encapsulation method used on the specified interfaces.
- The `ppp authentication pap dialins` command applies the “dialins” method list to the specified interfaces.

**Example: Configuring Login and Failed-Login Banners for AAA Authentication**

The following example shows how to configure a login banner that is displayed when a user logs in to the system, (in this case, the phrase “Unauthorized Access Prohibited”). The asterisk (*) is used as the delimiting character. RADIUS is specified as the default login authentication method.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```
This configuration displays the following login banner:

Unauthorized Access Prohibited
Username:

The following example shows how to configure a failed-login banner that is displayed when a user tries to log in to the system and fails, (in this case, the phrase “Failed login. Try again”). The asterisk (*) is used as the delimiting character. RADIUS is specified as the default login authentication method.

Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication fail-message *Failed login. Try again.*
Device(config)# aaa authentication login default group radius

This configuration displays the following login and failed-login banner:

Unauthorized Access Prohibited
Username:
Password:
Failed login. Try again.

Example: AAA Packet of Disconnect Server Key

The following example shows how to configure POD (packet of disconnect), which terminates connections on the network access server (NAS) when particular session attributes are identified.

aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop radius
aaa accounting delay-start
aaa pod server server-key xyz123
radius-server host 192.0.2.3 non-standard
radius-server key rad123

Example: Double Authentication

The examples in this section illustrate possible configurations to be used with double authentication. Your configurations could differ significantly, depending on your network and security requirements.

Note

These configuration examples include specific IP addresses and other specific information. This information is for illustration purposes only: your configuration will use different IP addresses, different usernames and passwords, and different authorization statements.

Example: Configuration of the Local Host for AAA with Double Authentication

These two examples show how to configure a local host to use AAA for PPP and login authentication, and for network and EXEC authorization. An example each is shown for RADIUS and for TACACS+.

In both the examples, the first three lines configure AAA with a specific server as the AAA server. The next two lines configure AAA for PPP and login authentication, and the last two lines configure network and EXEC
authorization. The last line is necessary only if the access-profile command will be executed as an autocommand.

The following example shows device configuration with a RADIUS AAA server:

```plaintext
aaa new-model
radius-server host secureserver
radius-server key myradiuskey
aaa authentication ppp default group radius
aaa authentication login default group radius
aaa authorization network default group radius
aaa authorization exec default group radius
```

The following example shows device configuration with a TACACS+ server:

```plaintext
aaa new-model
tacacs-server host security
tacacs-server key mytacacskey
aaa authentication ppp default group tacacs+
tacacs-server key mytacacskey
aaa authentication login default group tacacs+
tacacs-server key mytacacskey
aaa authorization network default group tacacs+
tacacs-server key mytacacskey
aaa authorization exec default group tacacs+
```

**Example: Configuration of the AAA Server for First-Stage PPP Authentication and Authorization**

This example shows a configuration on the AAA server. A partial sample AAA configuration is shown for RADIUS.

TACACS+ servers can be configured similarly. (See the Complete Configuration with TACACS Example.)

This example defines authentication/authorization for a remote host named “hostx” that will be authenticated by CHAP in the first stage of double authentication. Note that the ACL AV pair limits the remote host to Telnet connections to the local host. The local host has the IP address 10.0.0.2.

The following example shows a partial AAA server configuration for RADIUS:

```plaintext
hostx  Password = "welcome"
       User-Service-Type = Framed-User,
       Framed-Protocol = PPP,
       cisco-avpair = "lcp:interface-config-ip unnumbered fastethernet 0",
       cisco-avpair = "ip:inacl#3=permit tcp any 172.21.114.0 0.0.0.255 eq telnet",
       cisco-avpair = "ip:inacl#4=deny icmp any any",
       cisco-avpair = "ip:route#5=10.0.0.0 255.0.0.0",
       cisco-avpair = "ip:route#6=10.10.0.0 255.0.0.0",
       cisco-avpair = "ipx:inacl#3=deny any"
```

**Example: Configuration of the AAA Server for Second-Stage Per-User Authentication and Authorization**

This section contains partial sample AAA configurations on a RADIUS server. These configurations define authentication and authorization for a user (Pat) with the username “patuser,” who will be user-authenticated in the second stage of double authentication.

TACACS+ servers can be configured similarly. (See the Complete Configuration with TACACS Example.)

Three examples show sample RADIUS AAA configurations that could be used with each of the three forms of the access-profile command.

The first example shows a partial sample AAA configuration that works with the default form (no keywords) of the access-profile command. Note that only ACL AV pairs are defined. This example also sets up the access-profile command as an autocommand.
The second example shows a partial sample AAA configuration that works with the `access-profile merge` form of the `access-profile` command. This example also sets up the `access-profile merge` command as an autocommand.

```
patuser  Password = "welcome"
  User-Service-Type = Shell-User,
  cisco-avpair = "shell:autocmd=access-profile merge"
  User-Service-Type = Framed-User,
  Framed-Protocol = PPP,
  cisco-avpair = "ip:inacl#3=permit tcp any host 10.0.0.2 eq telnet",
  cisco-avpair = "ip:inacl#4=deny icmp any any"
```

The third example shows a partial sample AAA configuration that works with the `access-profile replace` form of the `access-profile` command. This example also sets up the `access-profile replace` command as an autocommand.

```
patuser  Password = "welcome"
  User-Service-Type = Shell-User,
  cisco-avpair = "shell:autocmd=access-profile replace"
  User-Service-Type = Framed-User,
  Framed-Protocol = PPP,
  cisco-avpair = "ip:inacl#3=permit tcp any any",
  cisco-avpair = "ip:route=10.10.0.0 255.255.0.0",
  cisco-avpair = "ip:route=10.11.0.0 255.255.0.0",
  cisco-avpair = "ip:route=10.12.0.0 255.255.0.0"
```

Example: Complete Configuration with TACACS

This example shows TACACS+ authorization profile configurations both for the remote host (used in the first stage of double authentication) and for specific users (used in the second stage of double authentication). This TACACS+ example contains approximately the same configuration information as shown in the previous RADIUS examples.

This sample configuration shows authentication/authorization profiles on the TACACS+ server for the remote host “hostx” and for three users, with the usernames “pat_default,” “pat_merge,” and “pat_replace.” The configurations for these three usernames illustrate different configurations that correspond to the three different forms of the `access-profile` command. The three user configurations also illustrate setting up the autocommand for each form of the `access-profile` command.

The figure below shows the topology. The example that follows the figure shows a TACACS+ configuration file.
This sample configuration shows authentication/authorization profiles on the TACACS+ server for the remote host “hostx” and for three users, with the usernames “pat_default,” “pat_merge,” and “pat_replace.”

```plaintext
key = "mytacacskey"
default authorization = permit
#-----------------------------Remote Host (BRI)-------------------------
# This allows the remote host to be authenticated by the local host
# during fist-stage authentication, and provides the remote host
# authorization profile.
#--------------------------------------------------------------------------------
user = hostx
  login = cleartext "welcome"
  chap = cleartext "welcome"
  service = exec
    {           # This is the autocommand that executes when pat_default logs in.
      autocmd = "access-profile"
    }

#------------------- "access-profile" default user "only acls" ------------------
# Without arguments, access-profile removes any access-lists it can find
# in the old configuration (both per-user and per-interface), and makes sure
# that the new profile contains ONLY access-list definitions.
#--------------------------------------------------------------------------------
user = pat_default
  login = cleartext "welcome"
  chap = cleartext "welcome"
  service = exec
    {
      autocmd = "access-profile"
    }
```

Figure 3: Example Topology for Double Authentication
service = ppp protocol = ip {
    # Put whatever access-lists, static routes, whatever
    # here.
    # If you leave this blank, the user will have NO IP
    # access-lists (not even the ones installed prior to
    # this)!
    inacl#3="permit tcp any host 10.0.0.2 eq telnet"
    inacl#4="deny icmp any any"
}

service = ppp protocol = ipx {
    # Put whatever access-lists, static routes, whatever
    # here.
    # If you leave this blank, the user will have NO IPX
    # access-lists (not even the ones installed prior to
    # this)!
}

#--------------------- "access-profile merge" user ---------------------------
#
# With the 'merge' option, first all old access-lists are removed (as before),
# but then (almost) all AV pairs are uploaded and installed. This will allow
# for uploading any custom static routes, sap-filters, and so on, that the user
# may need in his or her profile. This needs to be used with care, as it leaves
# open the possibility of conflicting configurations.
#
#--------------------- "access-profile replace" user ----------------------------
#
# With the 'replace' option, ALL old configuration is removed and ALL new
# configuration is installed.
#
# One caveat: access-profile checks the new configuration for address-pool and
# address AV pairs. As addresses cannot be renegotiated at this point, the
# command will fail (and complain) when it encounters such an AV pair.
Example: Automated Double Authentication

This example shows a complete configuration file with automated double authentication configured. The configuration commands that apply to automated double authentication are preceded by descriptions with a double asterisk (**).

Current configuration:

```ini
version 11.3
no service password-encryption
hostname myrouter

**The following AAA commands are used to configure double authentication:**

**The following command enables AAA:**
aaa new-model

**The following command enables user authentication via the RADIUS AAA server:**
aaa authentication login default none
aaa authentication ppp default group radius
```

**The following command causes the remote user’s authorization profile to be**
! downloaded from the AAA server to the router when required:
! aaa authorization network default group radius
! enable password mypassword
!
ip host blue 172.21.127.226
ip host green 172.21.127.218
ip host red 172.21.127.114
ip domain-name example.com
ip name-server 172.16.2.75
!
interface FastEthernet0/0/0
ip address 172.21.127.186 255.255.255.248
no ip route-cache
no ip mroute-cache
no keepalive
ntp disable
no cdp enable
!
interface Virtual-Template1
ip unnumbered loopback0
no ip route-cache
no ip mroute-cache
!
! **The following command specifies that device authentication occurs via PFP CHAP:
ppp authentication chap
!
router eigrp 109
network 172.21.0.0
no auto-summary
!
ip default-gateway 172.21.127.185
no ip classless
ip route 172.21.127.114 255.255.255.255 172.21.127.113
! **Virtual profiles are required for double authentication to work:
virtual-profile virtual-template 1
dialer-list 1 protocol ip permit
no cdp run
!
! **The following command defines where the TACACS+ AAA server is:
tacacs-server host 172.16.57.35 port 1049
tacacs-server timeout 90
! **The following command defines the key to use with TACACS+ traffic (required):
tacacs-server key mytacacsk ey
snmp-server community public RO
!
line con 0
exec-timeout 0 0
login authentication console
line aux 0
transport input all
line vty 0 4
exec-timeout 0 0
password lab
!
end

The lines in this sample RADIUS AAA configuration are defined as follows:

- The **aaa new-model** command enables AAA network security services.

- The **aaa authentication login admins local** command defines another method list, “admins”, for login authentication.
• The `aaa authentication ppp dialins group radius local` command defines the authentication method list “dialins,” which specifies that RADIUS authentication then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.

• The `aaa authorization network default group radius local` command is used to assign an address and other network parameters to the RADIUS user.

• The `aaa accounting network default start-stop group radius` command tracks PPP usage.

• The `username` command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.

• The `radius-server host` command defines the name of the RADIUS server host.

• The `radius-server key` command defines the shared secret text string between the network access server and the RADIUS server host.

• The `interface group-async` command selects and defines an asynchronous interface group.

• The `group-range` command defines the member asynchronous interfaces in the interface group.

• The `encapsulation ppp` command sets PPP as the encapsulation method used on the specified interfaces.

• The `ppp authentication ms-chap dialins` command selects MS-CHAP as the method of PPP authentication and applies the “dialins” method list to the specified interfaces.

• The `line` command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.

• The `autoselect ppp` command allows a PPP session to start up automatically on these selected lines.

• The `autoselect during-login` command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.

• The `login authentication admins` command applies the “admins” method list for login authentication.

• The `modem dialin` command configures modems attached to the selected lines to only accept incoming calls.

---

### Additional References for Configuring Authentication

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS commands</td>
<td><em>Cisco IOS Master Command List, All Releases</em></td>
</tr>
</tbody>
</table>

#### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1334</td>
<td>PPP Authentication Protocols</td>
</tr>
<tr>
<td>RFC 2433</td>
<td>Microsoft PPP CHAP Extensions</td>
</tr>
<tr>
<td>RFC 2903</td>
<td>Generic AAA Architecture</td>
</tr>
<tr>
<td>RFC 2904</td>
<td>AAA Authorization Framework</td>
</tr>
<tr>
<td>RFC 2906</td>
<td>AAA Authorization Requirements</td>
</tr>
<tr>
<td>RFC 2989</td>
<td>Criteria for Evaluating AAA Protocols for Network Access</td>
</tr>
</tbody>
</table>

Technical Assistance

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

Feature Information for Configuring Authentication

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Authentication</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>Authentication provides a method to identify users, which includes the login and password dialog, challenge and response, messaging support, and encryption, depending on the selected security protocol. Authentication is the way a user is identified prior to being allowed access to the network and network services.</td>
</tr>
</tbody>
</table>
Configuring Authorization

AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server 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. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it.

- AAA Authorization Prerequisites, on page 75
- Information About Configuring Authorization, on page 76
- How to Configure Authorization, on page 79
- Authorization Configuration Examples, on page 81
- Additional References for Configuring Authorization, on page 85
- Feature Information for Configuring Authorization, on page 85

AAA Authorization Prerequisites

Before configuring authorization using named method lists, you must first perform the following tasks:

- Enable AAA on your network access server.
- Configure AAA authentication. Authorization generally takes place after authentication and relies on authentication to work properly. For more information about AAA authentication, refer to the “Configuring Authentication” module.
- Define the characteristics of your RADIUS or TACACS+ security server if you are issuing RADIUS or TACACS+ authorization. For more information about configuring your Cisco network access server to communicate with your RADIUS security server, refer to the chapter “Configuring RADIUS”. For more information about configuring your Cisco network access server to communicate with your TACACS+ security server, refer to the “Configuring TACACS+” module.
- Define the rights associated with specific users by using the `username` command if you are issuing local authorization. For more information about the `username` command, refer to the Cisco IOS Security Command Reference.
Information About Configuring Authorization

Named Method Lists for Authorization

Method lists for authorization define the ways that authorization will be performed and the sequence in which these methods will be performed. A method list is simply a named list describing the authorization methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS XE software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS XE software selects the next method listed in the list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

Note

The Cisco IOS XE software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle--meaning that the security server or local username database responds by denying the user services--the authorization process stops and no other authorization methods are attempted.

Method lists are specific to the authorization type requested:

- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **EXEC**—Applies to the attributes associated with a user EXEC terminal session.
- **Network**—Applies to network connections. This can include a PPP, SLIP, or ARAP connection.
- **Reverse Access**—Applies to reverse Telnet sessions.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, method lists must be applied to specific lines or interfaces before any of the defined methods will be performed. The only exception is the default method list (which is named “default”). If the `aaa authorization` command for a particular authorization type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, local authorization takes place by default.

AAA Authorization Methods

AAA supports five different methods of authorization:

- **TACACS+**—The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.
Authorization Methods

To have the network access server request authorization information via a TACACS+ security server, use the `aaa authorization` command with the `group tacacs+` method keyword. For more specific information about configuring authorization using a TACACS+ security server, refer to the chapter “Configuring TACACS+.” For an example of how to enable a TACACS+ server to authorize the use of network services, including PPP and ARA, see the TACACS Authorization Examples.

To allow users to have access to the functions they request as long as they have been authenticated, use the `aaa authorization` command with the `if-authenticated` method keyword. If you select this method, all requested functions are automatically granted to authenticated users.

There may be times when you do not want to run authorization from a particular interface or line. To stop authorization activities on designated lines or interfaces, use the `none` method keyword. If you select this method, authorization is disabled for all actions.

To select local authorization, which means that the router or access server consults its local user database to determine the functions a user is permitted to use, use the `aaa authorization` command with the `local` method keyword. The functions associated with local authorization are defined by using the `username` global configuration command. For a list of permitted functions, refer to the chapter “Configuring Authentication.”

To have the network access server request authorization via a RADIUS security server, use the `radius` method keyword. For more specific information about configuring authorization using a RADIUS security server, refer to the chapter Configuring RADIUS. For an example of how to enable a RADIUS server to authorize services, see the RADIUS Authorization Example.
Authorization method lists for SLIP follow whatever is configured for PPP on the relevant interface. If no lists are defined and applied to a particular interface (or no PPP settings are configured), the default setting for authorization applies.

**Method Lists and Server Groups**

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers. R1 and R2 make up the group of RADIUS servers. T1 and T2 make up the group of TACACS+ servers.

Using server groups, you can specify a subset of the configured server hosts and use them for a particular service. For example, server groups allow you to define R1 and R2 as separate server groups, and T1 and T2 as separate server groups. This means you can specify either R1 and T1 in the method list or R2 and T2 in the method list, which provides more flexibility in the way that you assign RADIUS and TACACS+ resources.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different 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, authorization—the second host entry configured acts as fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

For more information about configuring server groups and about configuring server groups based on DNIS numbers, refer to the chapter Configuring RADIUS or the chapter Configuring TACACS+.

**AAA Authorization Types**

Cisco IOS XE software supports five different types of authorization:

- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **EXEC**—Applies to the attributes associated with a user EXEC terminal session.
- **Network**—Applies to network connections. This can include a PPP, SLIP, or ARAP connection.
- **Reverse Access**—Applies to reverse Telnet sessions.
- **Configuration**—Applies to downloading configurations from the AAA server.
- **IP Mobile**—Applies to authorization for IP mobile services.

**Authorization Types**

Named authorization method lists are specific to the indicated type of authorization.
To create a method list to enable authorization that applies specific security policies on a per-user basis, use the auth-proxy keyword. For detailed information on the authentication proxy feature, refer to the chapter “Configuring Authentication Proxy” in the “Traffic Filtering and Firewalls” part of this book.

To create a method list to enable authorization for all network-related service requests (including SLIP, PPP, PPP NCPs, and ARAP), use the network keyword.

To create a method list to enable authorization to determine if a user is allowed to run an EXEC shell, use the exec keyword.

To create a method list to enable authorization for specific, individual EXEC commands associated with a specific privilege level, use the commands keyword. (This allows you to authorize all commands associated with a specified command level from 0 to 15.)

To create a method list to enable authorization for reverse Telnet functions, use the reverse-access keyword.

For information about the types of authorization supported by the Cisco IOS XE software, refer to the AAA Authorization Types.

Authorization Attribute-Value Pairs

RADIUS and TACACS+ authorization both define specific rights for users by processing attributes, which are stored in a database on the security server. For both RADIUS and TACACS+, attributes are defined on the security server, associated with the user, and sent to the network access server where they are applied to the user’s connection.

For a list of supported RADIUS attributes, refer to the “RADIUS Attributes Overview and RADIUS IETF Attributes” chapter. For a list of supported TACACS+ AV pairs, refer to the “Configuring TACACS+” chapter.

How to Configure Authorization

Configuring AAA Authorization Using Named Method Lists

To configure AAA authorization using named method lists, use the following commands beginning in global configuration mode:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Device(config)# aaa authorization {auth-proxy</td>
<td>network</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Do one of the following: • Device(config)# line [aux</td>
<td>console</td>
</tr>
</tbody>
</table>
Disabling Authorization for Global Configuration Commands

The `aaa authorization` command with the keyword `commands` attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level. Because there are configuration commands that are identical to some EXEC-level commands, there can be some confusion in the authorization process. Using `no aaa authorization config-commands` stops the network access server from attempting configuration command authorization.

To disable AAA authorization for all global configuration commands, use the following command in global configuration mode:

```
Device(config)# no aaa authorization config-commands
```

To disable AAA authorization on the console, use the following command in global configuration mode:

```
Device(config)# no aaa authorization console
```

**Note**
AAA authorization is disabled on the console by default. If AAA authorization is enabled on the console, disable it by configuring the `no aaa authorization console` command during the AAA configuration stage. AAA should be disabled on the console for user authentication.

**Configuring Authorization for Reverse Telnet**

Telnet is a standard terminal emulation protocol used for remote terminal connection. Normally, you log in to a network access server (typically through a dialup connection) and then use Telnet to access other network devices from that network access server. There are times, however, when it is necessary to establish a reverse Telnet session. In reverse Telnet sessions, the Telnet connection is established in the opposite direction—from inside a network to a network access server on the network periphery to gain access to modems or other...
devices connected to that network access server. Reverse Telnet is used to provide users with dialout capability by allowing them to Telnet to modem ports attached to a network access server.

It is important to control access to ports accessible through reverse Telnet. Failure to do so could, for example, allow unauthorized users free access to modems where they can trap and divert incoming calls or make outgoing calls to unauthorized destinations.

Authentication during reverse Telnet is performed through the standard AAA login procedure for Telnet. Typically the user has to provide a username and password to establish either a Telnet or reverse Telnet session. Reverse Telnet authorization provides an additional (optional) level of security by requiring authorization in addition to authentication. When enabled, reverse Telnet authorization can use RADIUS or TACACS+ to authorize whether or not this user is allowed reverse Telnet access to specific asynchronous ports, after the user successfully authenticates through the standard Telnet login procedure.

Reverse Telnet authorization offers the following benefits:

- An additional level of protection by ensuring that users engaged in reverse Telnet activities are indeed authorized to access a specific asynchronous port using reverse Telnet.
- An alternative method (other than access lists) to manage reverse Telnet authorization.

To configure a network access server to request authorization information from a TACACS+ or RADIUS server before allowing a user to establish a reverse Telnet session, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# aaa authorization reverse-access method1 [method2 ...]</td>
<td>Configures the network access server to request authorization information before allowing a user to establish a reverse Telnet session.</td>
</tr>
</tbody>
</table>

This feature enables the network access server to request reverse Telnet authorization information from the security server, whether RADIUS or TACACS+. You must configure the specific reverse Telnet privileges for the user on the security server itself.

## Authorization Configuration Examples

### Example: TACACS Authorization

The following examples show how to use a TACACS+ server to authorize the use of network services, including PPP and ARA. If the TACACS+ server is not available or an error occurs during the authorization process, the fallback method (none) is to grant all authorization requests:

```
aaa authorization network default group tacacs+ none
```

The following example shows how to allow network authorization using TACACS+:

```
aaa authorization network default group tacacs+
```

The following example shows how to provide the same authorization, but it also creates address pools called "mci" and "att":

```
```
aaa authorization network default group tacacs+
ip address-pool local
ip local-pool mci 172.16.0.1 172.16.0.255
ip local-pool att 172.17.0.1 172.17.0.255

These address pools can then be selected by the TACACS daemon. A sample configuration of the daemon follows:

user = mci_customer1 {
    login = cleartext "some password"
    service = ppp protocol = ip {
        addr-pool=mci
    }
}
user = att_customer1 {
    login = cleartext "some other password"
    service = ppp protocol = ip {
        addr-pool=att
    }

Example: RADIUS Authorization

The following example shows how to configure the router to authorize using RADIUS:

aaa new-model
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
radius-server host ip
radius-server key

The lines in this sample RADIUS authorization configuration are defined as follows:

- The `aaa authorization exec default group radius if-authenticated` command configures the network access server to contact the RADIUS server to determine if users are permitted to start an EXEC shell when they log in. If an error occurs when the network access server contacts the RADIUS server, the fallback method is to permit the CLI to start, provided the user has been properly authenticated.

The RADIUS information returned may be used to specify an autocommand or a connection access list be applied to this connection.

- The `aaa authorization network default group radius` command configures network authorization via RADIUS. This can be used to govern address assignment, the application of access lists, and various other per-user quantities.

**Note** Because no fallback method is specified in this example, authorization will fail if, for any reason, there is no response from the RADIUS server.

Example: Reverse Telnet Authorization

The following examples show how to cause the network access server to request authorization information from a TACACS+ security server before allowing a user to establish a reverse Telnet session:
aaa new-model
aaa authentication login default group tacacs+
aaa authorization reverse-access default group tacacs+
!
tacacs-server host 172.31.255.0
tacacs-server timeout 90
tacacs-server key goaway

The lines in this sample TACACS+ reverse Telnet authorization configuration are defined as follows:

- The `aaa new-model` command enables AAA.
- The `aaa authentication login default group tacacs+` command specifies TACACS+ as the default method for user authentication during login.
- The `aaa authorization reverse-access default group tacacs+` command specifies TACACS+ as the method for user authorization when trying to establish a reverse Telnet session.
- The `tacacs-server host` command identifies the TACACS+ server.
- The `tacacs-server timeout` command sets the interval of time that the network access server waits for the TACACS+ server to reply.
- The `tacacs-server key` command defines the encryption key used for all TACACS+ communications between the network access server and the TACACS+ daemon.

The following example shows how to configure a generic TACACS+ server to grant a user, pat, reverse Telnet access to port tty2 on the network access server named “maple” and to port tty5 on the network access server named “oak”:

```
user = pat
login = cleartext lab
service = raccess {
  port#1 = maple/tty2
  port#2 = oak/tty5
}
```

**Note**

In this example, “maple” and “oak” are the configured host names of network access servers, not DNS names or alias.

The following example shows how to configure the TACACS+ server (CiscoSecure) to grant a user named pat reverse Telnet access:

```
user = pat
profile_id = 90
profile_cycle = 1
member = Tacacs_Users
service=shell {
  default cmd=permit
}
service=raccess {
  allow “c2511e0” “tty1” “.*”
  refuse “.*” “.*” “.*”
  password = clear “goaway”
  ```
CiscoSecure only supports reverse Telnet using the command line interface in versions 2.1(x) through version 2.2(1).

An empty “service=raccess {}” clause permits a user to have unconditional access to network access server ports for reverse Telnet. If no “service=raccess” clause exists, the user is denied access to any port for reverse Telnet.

For more information about configuring TACACS+, refer to the “Configuring TACACS” chapter. For more information about configuring CiscoSecure, refer to the *CiscoSecure Access Control Server User Guide*, version 2.1(2) or greater.

The following example shows how to cause the network access server to request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group radius
aaa authorization reverse-access default group radius
!
radius-server host 172.31.255.0
radius-server key go away
auth-port 1645 acct-port 1646
```

The lines in this sample RADIUS reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group radius** command specifies RADIUS as the default method for user authentication during login.
- The **aaa authorization reverse-access default group radius** command specifies RADIUS as the method for user authorization when trying to establish a reverse Telnet session.
- The **radius-server host** command identifies the RADIUS server.
- The **radius-server key** command defines the encryption key used for all RADIUS communications between the network access server and the RADIUS daemon.

The following example shows how to send a request to the RADIUS server to grant a user named “pat” reverse Telnet access at port tty2 on the network access server named “maple”:

```
Username = “pat”
Password = “goaway”
User-Service-Type = Shell-User
cisco-avpair = “raccess:port#1=maple/tty2”
```

The syntax "raccess:port=any/any" permits a user to have unconditional access to network access server ports for reverse Telnet. If no "raccess:port={nasname }/{tty number }” clause exists in the user profile, the user is denied access to reverse Telnet on all ports.

For more information about configuring RADIUS, refer to the chapter “Configuring RADIUS.”
Additional References for Configuring Authorization

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Master Command List, All Releases</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
<tr>
<td>download documentation, software, and tools. Use these resources to install</td>
<td></td>
</tr>
<tr>
<td>and configure the software and to troubleshoot and resolve technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies. Access to most tools on the Cisco</td>
<td></td>
</tr>
<tr>
<td>Support and Documentation website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information for Configuring Authorization

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 15: Feature Information for Configuring Authorization

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Authorization</td>
<td>Cisco IOS XE</td>
<td>AAA authorization enables you to limit the services available to a user. When AAA</td>
</tr>
<tr>
<td></td>
<td>Everest 16.6.1</td>
<td>authorization is enabled, the network access server uses information retrieved from</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the user’s profile, which is located either in the local user database or on the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>security server, to configure the user’s session. Once this is done, the user will</td>
</tr>
<tr>
<td></td>
<td></td>
<td>be granted access to a requested service only if the information in the user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>profile allows it.</td>
</tr>
</tbody>
</table>
Configuring Accounting

The AAA accounting feature allows the services that users are accessing and the amount of network resources that users are consuming to be tracked. When AAA accounting is enabled, the network access server reports user activity to the TACACS+ or RADIUS security server (depending on which security method is implemented) 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, and auditing.

- Prerequisites for Configuring Accounting, on page 87
- Restrictions for Configuring Accounting, on page 87
- Information About Configuring Accounting, on page 88
- How to Configure AAA Accounting, on page 101
- Configuration Examples for AAA Accounting, on page 109
- Additional References for Configuring Accounting, on page 113
- Feature Information for Configuring Accounting, on page 114

Prerequisites for Configuring Accounting

The following tasks must be performed before configuring accounting using named method lists:

- Enable AAA on the network access server by using the `aaa new-model` command in global configuration mode.

- Define the characteristics of the RADIUS or TACACS+ security server if RADIUS or TACACS+ authorization is issued. For more information about configuring the Cisco network access server to communicate with the RADIUS security server, see the Configuring RADIUS module. For more information about configuring the Cisco network access server to communicate with the TACACS+ security server, see the Configuring TACACS+ module.

Restrictions for Configuring Accounting

- Accounting information can be sent simultaneously to a maximum of only four AAA servers.

- For Service Selection Gateway (SSG) systems, the `aaa accounting network broadcast` command broadcasts only `start-stop` accounting records. If interim accounting records are configured using the
ssg accounting interval command, the interim accounting records are sent only to the configured default RADIUS server.

**Topic 2.1**

**Information About Configuring Accounting**

**Named Method Lists for Accounting**

Similar to authentication and authorization method lists, method lists for accounting define the way accounting is performed and the sequence in which these methods are performed.

Named accounting method lists allow particular security protocol to be designated and used on specific lines or interfaces for accounting services. The only exception is the default method list (which is named “default”). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list is simply a named list describing the accounting methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists allow one or more security protocols to be designated and used for accounting, thus ensuring a backup system for accounting in case the initial method fails. Cisco IOS software uses the first method listed to support accounting; if that method fails to respond, the Cisco IOS software selects the next accounting method listed in the method list. This process continues until there is successful communication with a listed accounting method, or all methods defined are exhausted.

**Note**

The Cisco IOS software attempts accounting with the next listed accounting method only when there is no response from the previous method. If accounting fails at any point in this cycle—meaning that the security server responds by denying the user access—the accounting process stops and no other accounting methods are attempted.

Accounting method lists are specific to the type of accounting being requested. AAA supports seven different types of accounting:

- **Network** --Provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.
- **EXEC** --Provides information about user EXEC terminal sessions of the network access server.
- **Commands** --Provides information about the EXEC mode commands that a user issues. Command accounting generates accounting records for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **Connection** --Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin.
- **System** --Provides information about system-level events.
- **Resource** --Provides “start” and “stop” records for calls that have passed user authentication, and provides “stop” records for calls that fail to authenticate.
- **VRRS** --Provides information about Virtual Router Redundancy Service (VRRS).
System accounting does not use named accounting lists; only the default list for system accounting can be defined.

Once again, when a named method list is created, a particular list of accounting methods for the indicated accounting type are defined.

Accounting method lists must be applied to specific lines or interfaces before any of the defined methods are performed. The only exception is the default method list (which is named “default”). If the `aaa accounting` command for a particular accounting type is issued without specifying a named method list, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined (a defined method list overrides the default method list). If no default method list is defined, then no accounting takes place.

This section includes the following subsections:

### Method Lists and Server Groups

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers. R1 and R2 comprise the group of RADIUS servers. T1 and T2 comprise the group of TACACS+ servers.

Cisco IOS software, RADIUS and TACACS+ server configurations are global. A subset of the configured server hosts can be specified using server groups. These server groups can be used for a particular service. For example, server groups allow R1 and R2 to be defined as separate server groups (SG1 and SG2), and T1 and T2 as separate server groups (SG3 and SG4). This means either R1 and T1 (SG1 and SG3) or R2 and T2 (SG2 and SG4) can be specified in the method list, which provides more flexibility in the way that RADIUS and TACACS+ resources are assigned.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server from 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 failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services (The RADIUS host entries are tried in the order in which they are configured).

For more information about configuring server groups and about configuring server groups based on Dialed Number Identification Service (DNIS) numbers, see the “Configuring RADIUS” or “Configuring TACACS+” module in the Cisco IOS Security Configuration Guide: Securing User Services.

### AAA Accounting Methods

The Cisco IOS software supports the following two methods for accounting:

- TACACS+- The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.
Accounting Record Types

- RADIUS--The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Note

With CSCuc32663, passwords and accounting logs are masked before being sent to the TACACS+ or RADIUS security servers. Use the `aaa accounting commands visible-keys` command to send unmasked information to the TACACS+ or RADIUS security servers.

Accounting Record Types

For minimal accounting, use the `stop-only` keyword, which instructs the specified method (RADIUS or TACACS+) to send a stop record accounting notice at the end of the requested user process. For more accounting information, use the `start-stop` keyword to send a start accounting notice at the beginning of the requested event and a stop accounting notice at the end of the event. To stop all accounting activities on this line or interface, use the `none` keyword.

Accounting Methods

The table below lists the supported accounting methods.

Table 16: AAA Accounting Methods

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group radius</code></td>
<td>Uses the list of all RADIUS servers for accounting.</td>
</tr>
<tr>
<td><code>group tacacs+</code></td>
<td>Uses the list of all TACACS+ servers for accounting.</td>
</tr>
<tr>
<td><code>group group-name</code></td>
<td>Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group <code>group-name</code>.</td>
</tr>
</tbody>
</table>

The method argument refers to the actual method the authentication algorithm tries. Additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all other methods return an error, specify additional methods in the command. For example, to create a method list named acct_tac1 that specifies RADIUS as the backup method of authentication in the event that TACACS+ authentication returns an error, enter the following command:

```
aaa accounting network acct_tac1 stop-only group tacacs+ group radius
```

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

For example, to specify RADIUS as the default method for user authentication during login, enter the following command:

```
aaa accounting network default stop-only group radius
```

AAA Accounting supports the following methods:

- `group tacacs` --To have the network access server send accounting information to a TACACS+ security server, use the `group tacacs+ method` keyword.
• **group radius** -- To have the network access server send accounting information to a RADIUS security server, use the `group radius` method keyword.

---

**Note**

Accounting method lists for SLIP follow whatever is configured for PPP on the relevant interface. If no lists are defined and applied to a particular interface (or no PPP settings are configured), the default setting for accounting applies.

• **group group-name** -- To specify a subset of RADIUS or TACACS+ servers to use as the accounting method, use the `aaa accounting` command with the `group group-name` method. To specify and define the group name and the members of the group, use the `aaa group server` command. For example, use the `aaa group server` command to first define the members of `group loginrad`:

```bash
aaa group server radius loginrad
server 172.16.2.3
server 172.16.2.17
server 172.16.2.32
```

This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the `group loginrad`.

To specify `group loginrad` as the method of network accounting when no other method list has been defined, enter the following command:

```bash
aaa accounting network default start-stop group loginrad
```

Before a group name can be used as the accounting method, communication with the RADIUS or TACACS+ security server must be enabled.

**AAA Accounting Types**

**Network Accounting**

Network accounting provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.

The following example shows the information contained in a RADIUS network accounting record for a PPP user who comes in through an EXEC session:

```plaintext
Wed Jun 27 04:44:45 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 5
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
  Caller-ID = "562"
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  Service-Type = Exec-User
  Acct-Session-Id = "0000000D"
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"
```

```plaintext
Wed Jun 27 04:45:00 2001
```
The following examples show the information contained in a TACACS+ network accounting record for a PPP user who first started an EXEC session:

Wed Jun 27 04:00:35 2001 172.16.25.15 username1 tty4 562/4327528 start
    task_id=28
    service=shell
Wed Jun 27 04:00:46 2001 172.16.25.15 username1 tty4 562/4327528 start
    task_id=30
    addr=10.1.1.1
    service=ppp
Thu Jun 27 04:00:49 2001 172.16.25.15 username1 tty4 408/4327528 update
    task_id=30
    addr=10.1.1.1
    service=ppp
    protocol=ip
    addr=10.1.1.1
Thu Jun 27 04:01:31 2001 172.16.25.15 username1 tty4 562/4327528 stop
    task_id=30
    addr=10.1.1.1
    service=ppp
    protocol=ip
    addr=10.1.1.1
Thu Jun 27 04:01:32 2001 172.16.25.15 username1 tty4 562/4327528 stop
    bytes_out=16382
    paks_out=24
    elapsed_time=51
    bytes_in=2844
    service=shell
    elapsed_time=57
The precise format of accounting packets records may vary depending on the security server daemon.

The following example shows the information contained in a RADIUS network accounting record for a PPP user who comes in through autoselect:

```
Wed Jun 27 04:30:52 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 3
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "0000000B"
Framed-Protocol = PPP
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 27 04:36:49 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 3
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "0000000B"
Framed-Protocol = PPP
Framed-IP-Address = "10.1.1.1"
Acct-Input-Octets = 8630
Acct-Output-Octets = 5722
Acct-Input-Packets = 94
Acct-Output-Packets = 64
Acct-Session-Time = 357
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```

The following example shows the information contained in a TACACS+ network accounting record for a PPP user who comes in through autoselect:

```
Wed Jun 27 04:02:19 2001 172.16.25.15 username1 Async5 562/4327528 start task_id=35
service=ppp
Wed Jun 27 04:02:25 2001 172.16.25.15 username1 Async5 562/4327528 update
task_id=35
service=ppp
protocol=ip
addr=10.1.1.2
Wed Jun 27 04:05:03 2001 172.16.25.15 username1 Async5 562/4327528 stoptask_id=35
service=ppp
protocol=ip
addr=10.1.1.2
bytes_in=3366
bytes_out=2149
paks_in=42
paks_out=28
elapsed_time=164
```

**EXEC Accounting**

EXEC accounting provides information about user EXEC terminal sessions (user shells) on the network access server, including username, date, start and stop times, the access server IP address, and (for dial-in users) the telephone number the call originated from.
The following example shows the information contained in a RADIUS EXEC accounting record for a dial-in user:

```
Wed Jun 27 04:26:23 2001
NAS-IP-Address = “172.16.25.15”
NAS-Port = 1
User-Name = “username1”
Client-Port-DNIS = “4327528”
Caller-ID = “5622329483”
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = “00000006”
Acct-Delay-Time = 0
User-Id = “username1”
NAS-Identifier = “172.16.25.15”
```

The following example shows the information contained in a TACACS+ EXEC accounting record for a dial-in user:

```
NAS-IP-Address = “172.16.25.15”
NAS-Port = 1
User-Name = “username1”
Client-Port-DNIS = “4327528”
Caller-ID = “5622329483”
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = “00000006”
Acct-Session-Time = 62
Acct-Delay-Time = 0
User-Id = “username1”
NAS-Identifier = “172.16.25.15”
```

The following example shows the information contained in a RADIUS EXEC accounting record for a Telnet user:

```
NAS-IP-Address = “172.16.25.15”
NAS-Port = 26
User-Name = “username1”
Caller-ID = “10.68.202.158”
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = “00000010”
Acct-Delay-Time = 0
User-Id = “username1”
NAS-Identifier = “172.16.25.15”
```

```
NAS-IP-Address = “172.16.25.15”
NAS-Port = 26
User-Name = “username1”
Caller-ID = “10.68.202.158”
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
```
Service-Type = Exec-User
Acct-Session-Id = "00000010"
Acct-Session-Time = 14
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

The following example shows the information contained in a TACACS+ EXEC accounting record for a Telnet user:

start task_id=41 service=shell
stop task_id=41 service=shell elapsed_time=9

Command Accounting

Command accounting provides information about the EXEC shell commands for a specified privilege level that are being executed on a network access server. Each command accounting record includes a list of the commands executed for that privilege level, as well as the date and time each command was executed, and the user who executed it.

The following example shows the information contained in a TACACS+ command accounting record for privilege level 1:

Wed Jun 27 03:46:47 2001 172.16.25.15 username1 tty3 562329430/4327528
stop task_id=3 service=shell priv-lvl=1 cmd=show version <cr>
Wed Jun 27 03:46:58 2001 172.16.25.15 username1 tty3 562329430/4327528
stop task_id=4 service=shell priv-lvl=1 cmd=show interfaces Ethernet 0 <cr>
Wed Jun 27 03:47:03 2001 172.16.25.15 username1 tty3 562329430/4327528
stop task_id=5 service=shell priv-lvl=1 cmd=show ip route <cr>

The following example shows the information contained in a TACACS+ command accounting record for privilege level 15:

Wed Jun 27 03:47:17 2001 172.16.25.15 username1 tty3 562329430/4327528
stop task_id=6 service=shell priv-lvl=15 cmd=configure terminal <cr>
Wed Jun 27 03:47:21 2001 172.16.25.15 username1 tty3 562329430/4327528
stop task_id=7 service=shell priv-lvl=15 cmd=interface Serial 0 <cr>
Wed Jun 27 03:47:29 2001 172.16.25.15 username1 tty3 562329430/4327528
stop task_id=8 service=shell priv-lvl=15 cmd-ip address 10.1.1.1 255.255.255.0 <cr>

Note

The Cisco implementation of RADIUS does not support command accounting.

Connection Accounting

Connection accounting provides information about all outbound connections made from the network access server such as Telnet, LAT, TN3270, PAD, and rlogin.

The following example shows the information contained in a RADIUS connection accounting record for an outbound Telnet connection:

Wed Jun 27 04:28:00 2001
The following example shows the information contained in a TACACS+ connection accounting record for an outbound Telnet connection:

```
Wed Jun 27 03:47:43 2001
172.16.25.15 username1 tty3 5622329430/4327528
start task_id=10 service=connection protocol=telnet addr=10.68.202.158 cmd=telnet
username1-sun
```

```
Wed Jun 27 03:48:38 2001
172.16.25.15 username1 tty3 5622329430/4327528
stop task_id=10 service=connection protocol=telnet addr=10.68.202.158 cmd=telnet
username1-sun bytes_in=4467 bytes_out=96 paks_in=61 paks_out=72 elapsed_time=55
```

The following example shows the information contained in a RADIUS connection accounting record for an outbound rlogin connection:

```
172.16.25.15 username1 tty3 5622329430/4327528
```

```
172.16.25.15 username1 tty3 5622329430/4327528
```

```
172.16.25.15 username1 tty3 5622329430/4327528
```

```
172.16.25.15 username1 tty3 5622329430/4327528
```

```
172.16.25.15 username1 tty3 5622329430/4327528
```

```
172.16.25.15 username1 tty3 5622329430/4327528
```

```
172.16.25.15 username1 tty3 5622329430/4327528
```

```
172.16.25.15 username1 tty3 5622329430/4327528
```
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:30:09 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "0000000A"
Login-Service = Rlogin
Login-IP-Host = "10.68.202.158"
Acct-Input-Octets = 18686
Acct-Output-Octets = 86
Acct-Input-Packets = 90
Acct-Output-Packets = 68
Acct-Session-Time = 22
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

The following examples show the information contained in a TACACS+ connection accounting record for an outbound rlogin connection:

Wed Jun 27 03:48:46 2001 172.16.25.15 username1 tty3 5622329430/4327528
start task_id=12 service=connection protocol=rlogin addr=10.68.202.158 cmd=rlogin
username1-sun /user username1
Wed Jun 27 03:51:37 2001 172.16.25.15 username1 tty3 5622329430/4327528
stop task_id=12 service=connection protocol=rlogin addr=10.68.202.158 cmd=rlogin
username1-sun /user username1 bytes_in=659926 bytes_out=138 paks_in=2378 paks_out=1251 elapsed_time=171

The following examples show the information contained in a TACACS+ connection accounting record for an outbound LAT connection:

Wed Jun 27 03:53:06 2001 172.16.25.15 username1 tty3 5622329430/4327528
start task_id=18 service=connection protocol=lat addr=VAX cmd=lat
VAX
Wed Jun 27 03:54:15 2001 172.16.25.15 username1 tty3 5622329430/4327528
stop task_id=18 service=connection protocol=lat addr=VAX cmd=lat
VAX bytes_in=0 bytes_out=0 paks_in=0 paks_out=0 elapsed_time=6

System Accounting

System accounting provides information about all system-level events (for example, when the system reboots or when accounting is turned on or off).

The following accounting record shows a typical TACACS+ system accounting record server indicating that AAA Accounting has been turned off:

service=system event=sys_acct reason=reconfigure

Note

The precise format of accounting packets records may vary depending on the TACACS+ daemon.
The following accounting record shows a TACACS+ system accounting record indicating that AAA Accounting has been turned on:

```plaintext
Wed Jun 27 03:55:22 2001 172.16.25.15 unknown unknown unknown stop task_id=23
   service-system event=sys_acct reason=reconfigure
```

Additional tasks for measuring system resources are covered in the Cisco IOS software configuration guides. For example, IP accounting tasks are described in the Configuring IP Services chapter in the *Cisco IOS Application Services Configuration Guide*.

## Resource Accounting

The Cisco implementation of AAA accounting provides “start” and “stop” record support for calls that have passed user authentication. The additional feature of generating “stop” records for calls that fail to authenticate as part of user authentication is also supported. Such records are necessary for users employing accounting records to manage and monitor their networks.

This section includes the following subsections:

### AAA Resource Failure Stop Accounting

Before AAA resource failure stop accounting, there was no method of providing accounting records for calls that failed to reach the user authentication stage of a call setup sequence. Such records are necessary for users employing accounting records to manage and monitor their networks and their wholesale customers.

This functionality generates a “stop” accounting record for any calls that do not reach user authentication; “stop” records are generated from the moment of call setup. All calls that pass user authentication behave as they did before; that is, no additional accounting records are seen.

The figure below illustrates a call setup sequence with normal call flow (no disconnect) and without AAA resource failure stop accounting enabled.

**Figure 4: Modem Dial-In Call Setup Sequence With Normal Flow and Without Resource Failure Stop Accounting Enabled**

![Call Setup Sequence Diagram](image)

The figure below illustrates a call setup sequence with normal call flow (no disconnect) and with AAA resource failure stop accounting enabled.
AAA Resource Accounting for Start-Stop Records

AAA resource accounting for start-stop records supports the ability to send a “start” record at each call setup, followed by a corresponding “stop” record at the call disconnect. This functionality can be used to manage and monitor wholesale customers from one source of data reporting, such as accounting records.

With this feature, a call setup and call disconnect “start-stop” accounting record tracks the progress of the resource connection to the device. A separate user authentication “start-stop” accounting record tracks the user management progress. These two sets of accounting records are interlinked by using a unique session ID for the call.

The figure below illustrates a call setup sequence with AAA resource start-stop accounting enabled.
AAA Accounting Enhancements

AAA Broadcast Accounting

AAA broadcast accounting allows accounting information to be sent to multiple AAA servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows service providers to send accounting information to their own private AAA servers and to the AAA servers of their end customers. It also provides redundant billing information for voice applications.

Broadcasting is allowed among groups of RADIUS or TACACS+ servers, and each server group can define its backup servers for failover independently of other groups.

Thus, service providers and their end customers can use different protocols (RADIUS or TACACS+) for the accounting server. Service providers and their end customers can also specify their backup servers independently. As for voice applications, redundant accounting information can be managed independently through a separate group with its own failover sequence.

AAA Session MIB

The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using Simple Network Management Protocol (SNMP). The data of the client is presented so that it correlates directly to the AAA Accounting information reported by either the RADIUS or the TACACS+ server. AAA session MIB provides the following information:

- Statistics for each AAA function (when used in conjunction with the `show radius statistics` command)
- Status of servers providing AAA functions
- Identities of external AAA servers
- Real-time information (such as idle times), providing additional criteria for use by SNMP networks for assessing whether or not to terminate an active call

**Note**

This command is supported only on Cisco AS5300 and Cisco AS5800 universal access server platforms.

The table below shows the SNMP user-end data objects that can be used to monitor and terminate authenticated client connections with the AAA session MIB feature.
Table 17: SNMP End-User Data Objects

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sessionId</td>
<td>The session identification used by the AAA Accounting protocol (same value as reported by RADIUS attribute 44 (Acct-Session-ID)).</td>
</tr>
<tr>
<td>userId</td>
<td>The user login ID or zero-length string if a login is unavailable.</td>
</tr>
<tr>
<td>ipAddr</td>
<td>The IP address of the session or 0.0.0.0 if an IP address is not applicable or unavailable.</td>
</tr>
<tr>
<td>idleTime</td>
<td>The elapsed time in seconds that the session has been idle.</td>
</tr>
<tr>
<td>disconnect</td>
<td>The session termination object used to disconnect the given client.</td>
</tr>
<tr>
<td>callId</td>
<td>The entry index corresponding to this accounting session that the Call Tracker record stored.</td>
</tr>
</tbody>
</table>

The table below describes the AAA summary information provided by the AAA session MIB feature using SNMP on a per-system basis.

Table 18: SNMP AAA Session Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activeTableEntries</td>
<td>Number of sessions currently active.</td>
</tr>
<tr>
<td>activeTableHighWaterMark</td>
<td>Maximum number of sessions present at once since last system reinstallation.</td>
</tr>
<tr>
<td>totalSessions</td>
<td>Total number of sessions since last system reinstallation.</td>
</tr>
<tr>
<td>disconnectedSessions</td>
<td>Total number of sessions that have been disconnected using since last system reinstallation.</td>
</tr>
</tbody>
</table>

Accounting Attribute-Value Pairs

The network access server monitors the accounting functions defined in either TACACS+ AV pairs or RADIUS attributes, depending on which security method is implemented.

How to Configure AAA Accounting

Configuring AAA Accounting Using Named Method Lists

To configure AAA Accounting using named method lists, perform the following steps:

**Note**

System accounting does not use named method lists. For system accounting, define only the default method list.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates an accounting method list and enables accounting. The argument <em>list-name</em> is a character string used to name the created list.</td>
<td></td>
</tr>
<tr>
<td>aaa accounting {system</td>
<td>network</td>
<td>exec</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# aaa accounting system default start-stop</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enters the line configuration mode for the lines to which the accounting method list is applied. or Enters the interface configuration mode for the interfaces to which the accounting method list is applied.</td>
<td></td>
</tr>
<tr>
<td>Do one of the following:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• line [aux</td>
<td>console</td>
<td>tty</td>
</tr>
<tr>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• interface interface-type interface-number</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# line aux line1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Applies the accounting method list to a line or set of lines. or Applies the accounting method list to an interface or set of interfaces.</td>
<td></td>
</tr>
<tr>
<td>Do one of the following:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• accounting {arap</td>
<td>commands level</td>
<td>connection</td>
</tr>
<tr>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ppp accounting {default</td>
<td>list-name}</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-line)# accounting arap default</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Exits line configuration mode and returns to global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-line)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What to do next

This section includes the following subsection:

Suppressing Generation of Accounting Records for Null Username Sessions

When AAA Accounting is activated, the Cisco IOS software issues accounting records for all users on the system, including users whose username string, because of protocol translation, is NULL. An example of this is users who come in on lines where the `aaa authentication login method-list none` command is applied. To prevent accounting records from being generated for sessions that do not have usernames associated with them, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# aaa accounting suppress null-username</td>
<td>Prevents accounting records from being generated for users whose username string is NULL.</td>
</tr>
</tbody>
</table>

Generating Interim Accounting Records

To enable periodic interim accounting records to be sent to the accounting server, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# aaa accounting update [newinfo] [periodic] number</td>
<td>Enables periodic interim accounting records to be sent to the accounting server.</td>
</tr>
</tbody>
</table>

When the `aaa accounting update` command is activated, the Cisco IOS software issues interim accounting records for all users on the system. If the keyword `newinfo` is used, interim accounting records are sent to the accounting server every time there is new accounting information to report. An example of this would be when IPCP completes IP address negotiation with the remote peer. The interim accounting record includes the negotiated IP address used by the remote peer.

When used with the keyword `periodic`, interim accounting records are sent periodically as defined by the `number` argument. The interim accounting record contains all of the accounting information recorded for that user up to the time the interim accounting record is sent.

Caution

Using the `aaa accounting update periodic` command can cause heavy congestion when many users are logged in to the network.

Configuring an Alternate Method to Enable Periodic Accounting Records

You can use the following alternative method to enable periodic interim accounting records to be sent to the accounting server.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  Example: Router> enable  
  • Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal |
| **Step 3** aaa accounting network default | Configures the default accounting for all network-related service requests and enters accounting method list configuration mode. |
| **Example:** Router(config)# aaa accounting network default |
| **Step 4** action-type \{none | start-stop \[periodic \{disable | interval minutes\}\] | stop-only\} | Specifies the type of action to be performed on accounting records.  
  \* (Optional) The periodic keyword specifies periodic accounting action.  
  • The interval keyword specifies the periodic accounting interval.  
  • The value argument specifies the intervals for accounting update records (in minutes).  
  • The disable keyword disables periodic accounting. |
| **Example:** Router(cfg-acct-mlist)# action-type start-stop  
  **Example:** periodic interval 5 |
| **Step 5** exit | Returns to global configuration mode. |
| **Example:** Router(cfg-acct-mlist)# exit |

### Generating Interim Service Accounting Records

Perform this task to enable the generation of interim service accounting records at periodic intervals for subscribers.

**Before you begin**

RADIUS Attribute 85 in the user service profile always takes precedence over the configured interim-interval value. RADIUS Attribute 85 must be in the user service profile. See the RADIUS Attributes Overview and RADIUS IETF Attributes feature document for more information.
If RADIUS Attribute 85 is not in the user service profile, then the interim-interval value configured in Generating Interim Accounting Records is used for service interim accounting records.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
<td><img src="" alt=" " /></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
<td><img src="" alt=" " /></td>
</tr>
<tr>
<td>Step 3</td>
<td>subscriber service accounting interim-interval minutes</td>
<td>Enables the generation of interim service accounting records at periodic intervals for subscribers. The minutes argument indicates the number of periodic intervals to send accounting update records from 1 to 71582 minutes.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# subscriber service accounting interim-interval 10</td>
<td><img src="" alt=" " /></td>
</tr>
</tbody>
</table>

### Generating Accounting Records for a Failed Login or Session

When AAA accounting is activated, the Cisco IOS XE software does not generate accounting records for system users who fail login authentication, or who succeed in login authentication but fail PPP negotiation for some reason.

To specify that accounting stop records be generated for users who fail to authenticate at login or during session negotiation, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting send stop-record authentication failure</td>
<td>Generates “stop” records for users who fail to authenticate at login or during session negotiation using PPP.</td>
</tr>
</tbody>
</table>

### Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records

For PPP users who start EXEC terminal sessions, it can be specified that NETWORK records be generated before EXEC-stop records. In some cases, such as billing customers for specific services, is can be desirable to keep network start and stop records together, essentially “nesting” them within the framework of the EXEC start and stop messages. For example, a user dialing in using PPP can create the following records: EXEC-start, NETWORK-start, EXEC-stop, NETWORK-stop. By nesting the network accounting records, NETWORK-stop records follow NETWORK-start messages: EXEC-start, NETWORK-start, NETWORK-stop, EXEC-stop.
To nest accounting records for user sessions, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa accounting nested</code></td>
<td>Nests network accounting records.</td>
</tr>
</tbody>
</table>

**Suppressing System Accounting Records over Switchover**

To suppress the system accounting-on and accounting-off messages during switchover, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa accounting redundancy suppress system-records</code></td>
<td>Suppresses the system accounting messages during switchover.</td>
</tr>
</tbody>
</table>

**Configuring AAA Resource Failure Stop Accounting**

To enable resource failure stop accounting, use the following command in global configuration mode:

```
Device(config)# aaa accounting resource method-list stop-failure group server-group
```

**Note**

Before configuring this feature, the tasks described in the Prerequisites for Configuring Accounting, on page 87 section must be performed, and SNMP must be enabled on the network access server. For more information about enabling SNMP on a Cisco router or access server, see the Configuring SNMP Support chapter in the Cisco IOS Network Management Configuration Guide.

**Configuring AAA Resource Accounting for Start-Stop Records**

To enable full resource accounting for start-stop records, use the following command in global configuration mode:

```
### AAA Broadcast Accounting

AAA broadcast accounting allows accounting information to be sent to multiple AAA servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows service providers to send accounting information to their own private AAA servers and to the AAA servers of their end customers. It also provides redundant billing information for voice applications.

Broadcasting is allowed among groups of RADIUS or TACACS+ servers, and each server group can define its backup servers for failover independently of other groups.

Thus, service providers and their end customers can use different protocols (RADIUS or TACACS+) for the accounting server. Service providers and their end customers can also specify their backup servers independently. As for voice applications, redundant accounting information can be managed independently through a separate group with its own failover sequence.

### Configuring Per-DNIS AAA Broadcast Accounting

To configure AAA broadcast accounting per DNIS, use the `aaa dnis map accounting network` command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Device(config)# aaa dnis map 
dnis-number  accounting network 
[\|start-stop | stop-only | none\|broadcast] method1 [method2... ] | Allows per-DNIS accounting configuration. This command has precedence over the global **aaa accounting** command. Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group. |

### AAA Session MIB

The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using Simple Network Management Protocol (SNMP). The data of the client is presented so that it correlates directly to the AAA Accounting information reported by either the RADIUS or the TACACS+ server. AAA session MIB provides the following information:
• Statistics for each AAA function (when used in conjunction with the `show radius statistics` command)
• Status of servers providing AAA functions
• Identities of external AAA servers
• Real-time information (such as idle times), providing additional criteria for use by SNMP networks for assessing whether or not to terminate an active call

**Note**
This command is supported only on Cisco AS5300 and Cisco AS5800 universal access server platforms.

The table below shows the SNMP user-end data objects that can be used to monitor and terminate authenticated client connections with the AAA session MIB feature.

**Table 19: SNMP End-User Data Objects**

<table>
<thead>
<tr>
<th>SessionId</th>
<th>The session identification used by the AAA Accounting protocol (same value as reported by RADIUS attribute 44 (Acct-Session-ID)).</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserId</td>
<td>The user login ID or zero-length string if a login is unavailable.</td>
</tr>
<tr>
<td>IpAddr</td>
<td>The IP address of the session or 0.0.0.0 if an IP address is not applicable or unavailable.</td>
</tr>
<tr>
<td>IdleTime</td>
<td>The elapsed time in seconds that the session has been idle.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>The session termination object used to disconnect the given client.</td>
</tr>
<tr>
<td>CallId</td>
<td>The entry index corresponding to this accounting session that the Call Tracker record stored.</td>
</tr>
</tbody>
</table>

The table below describes the AAA summary information provided by the AAA session MIB feature using SNMP on a per-system basis.

**Table 20: SNMP AAA Session Summary**

<table>
<thead>
<tr>
<th>ActiveTableEntries</th>
<th>Number of sessions currently active.</th>
</tr>
</thead>
</table>
| ActiveTableHighWaterMark | Maximum number of sessions present at once since last system reinstalla|}

| TotalSessions | Total number of sessions since last system reinstalla|}

| DisconnectedSessions | Total number of sessions that have been disconnected using since last system reinstalla|}

**Establishing a Session with a Router if the AAA Server Is Unreachable**

To establish a console session with a router if the AAA server is unreachable, use the following command in global configuration mode:
The `no aaa accounting system guarantee-first` command guarantees system accounting as the first record, which is the default condition. In some situations, users may be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than three minutes. To resolve this problem, use the `no aaa accounting system guarantee-first` command.

### Monitoring Accounting

No specific `show` command exists for either RADIUS or TACACS+ accounting. To obtain accounting records displaying information about users logged in, use the following command in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show accounting</code></td>
<td>Allows display of the active accountable events on the network and helps collect information in the event of a data loss on the accounting server.</td>
</tr>
</tbody>
</table>

### Troubleshooting Accounting

To troubleshoot accounting information, use the following command in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug aaa accounting</code></td>
<td>Displays information on accountable events as they occur.</td>
</tr>
</tbody>
</table>

### Configuration Examples for AAA Accounting

#### Example: Configuring a Named Method List

The following example shows how to configure a Cisco AS5200 (enabled for AAA and communication with a RADIUS security server) in order for AAA services to be provided by the RADIUS server. If the RADIUS server fails to respond, then the local database is queried for authentication and authorization information, and accounting services are handled by a TACACS+ server.

```plaintext
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network network1 group radius local
aaa accounting network network2 start-stop group radius group tacacs+
username root password ALongPassword
  tacacs-server host 172.31.255.0
  tacacs-server key goaway
radius-server host 172.16.2.7
  radius-server key myRaDiUSpassWoRd
interface group-async 1
  group-range 1 16
```

Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)
The lines in this sample RADIUS AAA configuration are defined as follows:

- The `aaa new-model` command enables AAA network security services.

- The `aaa authentication login admins local` command defines a method list, “admins”, for login authentication.

- The `aaa authentication ppp dialins group radius local` command defines the authentication method list “dialins”, which specifies that first RADIUS authentication and then (if the RADIUS server does not respond) local authentication is used on serial lines using PPP.

- The `aaa authorization network network1 group radius local` command defines the network authorization method list named “network1”, which specifies that RADIUS authorization is used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization is performed.

- The `aaa accounting network network2 start-stop group radius group tacacs+` command defines the network accounting method list named “network2”, which specifies that RADIUS accounting services (in this case, start and stop records for specific events) are used on serial lines using PPP. If the RADIUS server fails to respond, accounting services are handled by a TACACS+ server.

- The `username` command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.

- The `tacacs-server host` command defines the name of the TACACS+ server host.

- The `tacacs-server key` command defines the shared secret text string between the network access server and the TACACS+ server host.

- The `radius-server host` command defines the name of the RADIUS server host.

- The `radius-server key` command defines the shared secret text string between the network access server and the RADIUS server host.

- The `interface group-async` command selects and defines an asynchronous interface group.

- The `group-range` command defines the member asynchronous interfaces in the interface group.

- The `encapsulation ppp` command sets PPP as the encapsulation method used on the specified interfaces.

- The `ppp authentication chap dialins` command selects Challenge Handshake Authentication Protocol (CHAP) as the method of PPP authentication and applies the “dialins” method list to the specified interfaces.

- The `ppp authorization network1` command applies the blue1 network authorization method list to the specified interfaces.

- The `ppp accounting network2` command applies the red1 network accounting method list to the specified interfaces.
• The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.

• The **autoselect ppp** command configures the Cisco IOS XE software to allow a PPP session to start up automatically on these selected lines.

• The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.

• The **login authentication admins** command applies the admins method list for login authentication.

• The **modem dialin** command configures modems attached to the selected lines to accept only incoming calls.

The **show accounting** command yields the following output for the preceding configuration:

```
Active Accounted actions on tty1, User username2 Priv 1
Task ID 5, Network Accounting record, 00:00:52 Elapsed
task_id=5 service=ppp protocol=ip address=10.0.0.98
```

The table below describes the fields contained in the preceding output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Accounted actions on</td>
<td>Terminal line or interface name user with which the user logged in.</td>
</tr>
<tr>
<td>User</td>
<td>User’s ID.</td>
</tr>
<tr>
<td>Priv</td>
<td>User’s privilege level.</td>
</tr>
<tr>
<td>Task ID</td>
<td>Unique identifier for each accounting session.</td>
</tr>
<tr>
<td>Accounting Record</td>
<td>Type of accounting session.</td>
</tr>
<tr>
<td>Elapsed</td>
<td>Length of time (hh:mm:ss) for this session type.</td>
</tr>
<tr>
<td>attribute=value</td>
<td>AV pairs associated with this accounting session.</td>
</tr>
</tbody>
</table>

**Example: Configuring AAA Resource Accounting**

The following example shows how to configure the resource failure stop accounting and resource accounting for start-stop records functions:

```
!Enable AAA on your network access server.
aaa new-model
!Enable authentication at login and list the AOL string name to use for login authentication.
aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
aaa authentication ppp default group radius local
!Enable authorization for all exec sessions and list the AOL string name to use for authorization.
aaa authorization exec AOL group radius if-authenticated
!Enable authorization for all network-related service requests and list the default method to use for all network-related authorizations.
```
aaa authorization network default group radius if-authenticated
!Enable accounting for all exec sessions and list the default method to use for all start-stop
accounting services.

aaa accounting exec default start-stop group radius
!Enable accounting for all network-related service requests and list the default method to
use for all start-stop accounting services.

aaa accounting network default start-stop group radius
!Enable failure stop accounting.

aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.

aaa accounting resource default start-stop group radius

Example: Configuring AAA Broadcast Accounting

The following example shows how to turn on broadcast accounting using the global aaa accounting command:

```sh
aaa group server radius isp
    server 10.0.0.1
    server 10.0.0.2
aaa group server tacacs+ isp_customer
    server 172.0.0.1
aaa accounting network default start-stop broadcast group isp group isp_customer
    radius-server host 10.0.0.1
    radius-server host 10.0.0.2
    radius-server key key1
    tacacs-server host 172.0.0.1 key key2
```

The broadcast keyword causes “start” and “stop” accounting records for network connections to be sent simultaneously to server 10.0.0.1 in the group isp and to server 172.0.0.1 in the group isp_customer. If server 10.0.0.1 is unavailable, failover to server 10.0.0.2 occurs. If server 172.0.0.1 is unavailable, no failover occurs because backup servers are not configured for the group isp_customer.

Example: Configuring per-DNIS AAA Broadcast Accounting

The following example shows how to turn on per-DNIS broadcast accounting using the global aaa dnis map accounting network command:

```sh
aaa group server radius isp
    server 10.0.0.1
    server 10.0.0.2
aaa group server tacacs+ isp_customer
    server 172.0.0.1
aaa dnis map enable
aaa dnis map 7777 accounting network start-stop broadcast group isp group isp_customer
    radius-server host 10.0.0.1
    radius-server host 10.0.0.2
    radius-server key key_1
    tacacs-server host 172.0.0.1 key key_2
```

The broadcast keyword causes “start” and “stop” accounting records for network connection calls having DNIS number 7777 to be sent simultaneously to server 10.0.0.1 in the group isp and to server 172.0.0.1 in the group isp_customer. If server 10.0.0.1 is unavailable, failover to server 10.0.0.2 occurs. If server 172.0.0.1 is unavailable, no failover occurs because backup servers are not configured for the group isp_customer.
Example: AAA Session MIB

The following example shows how to set up the AAA session MIB feature to disconnect authenticated client connections for PPP users:

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
aaa session-mib disconnect
```

Additional References for Configuring Accounting

The following sections provide references related to the Configuring Accounting feature.

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
</tbody>
</table>

**MIBs**

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

**RFCs**

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
</tr>
</tbody>
</table>
Technical Assistance

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

Feature Information for Configuring Accounting

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Broadcast Accounting</td>
<td></td>
<td>AAA broadcast accounting allows accounting information to be sent to multiple AAA servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously.</td>
</tr>
<tr>
<td>AAA Session MIB</td>
<td></td>
<td>The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using Simple Network Management Protocol (SNMP).</td>
</tr>
<tr>
<td>Connection Accounting</td>
<td></td>
<td>Connection accounting provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin.</td>
</tr>
<tr>
<td>AAA Interim Accounting</td>
<td></td>
<td>AAA interim accounting allows accounting records to be sent to the accounting server every time there is new accounting information to report, or on a periodic basis.</td>
</tr>
</tbody>
</table>
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:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable`   | Enables privileged EXEC mode.  
|       | Example:     | • Enter your password if prompted.   |
|       | `Device> enable` |         |
### Command or Action | Purpose
--- | ---
**Step 2** configure terminal  
Example:  
Device# configure terminal | Enters global configuration mode.

**Step 3** aaa new-model  
Example:  
Device(config)# aaa new-model | Enables AAA.

**Step 4** aaa authentication login default local  
Example:  
Device(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.

**Step 5** aaa authorization exec default local  
Example:  
Device(config)# aaa authorization exec default local | Configures user AAA authorization, check the local database, and allow the user to run an EXEC shell.

**Step 6** aaa authorization network default local  
Example:  
Device(config)# aaa authorization network default local | Configures user AAA authorization for all network-related service requests.

**Step 7** username name [privilege level] {password encryption-type password}  
Example:  
Device(config)# username your_user_name privilege 1 password 7 secret567 | Enters the local database, and establishes a username-based authentication system. Repeat this command for each user.

- For name, specify the user ID as one word. Spaces and quotation marks are not allowed.
- (Optional) For level, specify the privilege level the user has after gaining access. The range is 0 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.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Enter 7 to specify that a hidden password follows.  
• For password, specify the password the user must enter to gain access to the switch. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the `username` command. | |
| Step 8 end | Returns to privileged EXEC mode. |
| Example: 
Device(config)# end | |
| Step 9 `show running-config` | Verifies your entries. |
| Example: 
Device# `show running-config` | |
| Step 10 `copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |
| Example: 
Device# `copy running-config startup-config` | |

**Monitoring Local Authentication and Authorization**

To display Local Authentication and Authorization configuration, use the `show running-config` privileged EXEC command.

**Additional References**

**Error Message Decoder**

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

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

Technical Assistance

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

Feature Information for Local Authentication and Authorization

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature. Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Authentication and Authorization</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Prerequisites for TACACS+

The following are the prerequisites for setup and configuration of switch access with TACACS+ (must be performed in the order presented):

1. Configure the switches with the TACACS+ server addresses.
2. Set an authentication key.
3. Configure the key from Step 2 on the TACACS+ servers.
4. Enable authentication, authorization, and accounting (AAA).
5. Create a login authentication method list.
6. Apply the list to the terminal lines.
7. Create an authorization and accounting method list.

The following are the prerequisites for controlling switch access with TACACS+:

- You must have access to a configured TACACS+ server to configure TACACS+ features on your switch. Also, you must have access to TACACS+ services maintained in a database on a TACACS+ daemon typically running on a LINUX or Windows workstation.
- 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+.

## Information About Controlling Switch Access with 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.

### 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—individually, 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.
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.

## 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

### 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.

If a method list is configured under VTY lines, the corresponding method list must be added to AAA. The following example shows how to configure a method list under a VTY line:

```
Device# configure terminal
Device(config)# line vty 0 4
Device(config)# authorization commands 15 auth1
```

The following example shows how to configure a method list in AAA:

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 auth1 group tacacs+
```
If no method list is configured under VTY lines, the default method list must be added to AAA. The following example shows a VTY configuration without a method list:

Device# configure terminal
Device(config)# line vty 0 4

The following example shows how to configure the default method list:

Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 default group tacacs+

**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.

**TACACS+ Login Authentication**

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

**TACACS+ Authorization for Privileged EXEC Access and Network Services**

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch uses information retrieved from the user’s profile, which is located either in the local user database or on the security server, to configure the user’s session. The user is granted access to a requested service only if the information in the user profile allows it.

**TACACS+ Accounting**

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the switch reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

**Default TACACS+ Configuration**

TACACS+ and AAA are disabled by default.
To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate users accessing the switch through the CLI.

**Note**
Although TACACS+ configuration is performed through the CLI, the TACACS+ server authenticates HTTP connections that have been configured with a privilege level of 15.

### How to Configure Switch Access with TACACS+

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

#### Identifying the TACACS+ Server Host and Setting the Authentication Key

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

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>tacacs server server-name</td>
<td>Identifies the IP host or hosts maintaining a TACACS+ server. Enter this command multiple times to create a list of preferred hosts. The software searches for hosts in the order in which you specify them. For server-name, specify the server name.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>tacacs server yourserver</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>address {ipv4</td>
<td>ipv6} ip address</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>address ipv4 10.0.1.12</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>exit</td>
<td>Exits the TACACS server mode and enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring TACACS+ Login Authentication

Follow these steps to configure TACACS+ login authentication:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td><code>aaa new-model</code></td>
<td>Enables AAA.</td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# aaa new-model</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>aaa group server tacacs+ group-name</code></td>
<td>(Optional) Defines the AAA server-group with a group name. This command puts the Device in a server group subconfiguration mode.</td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# aaa group server tacacs+ your_server_group</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>server ip-address</code></td>
<td>(Optional) Associates a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group. Each server in the group must be previously defined in Step 3.</td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# server 10.1.2.3</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# end</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td><code>Device# show running-config</code></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td><code>Device# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
### 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 for HTTP access by using AAA methods, you must configure the with the `ip http authentication aaa` global configuration command. Configuring AAA authentication does not secure the 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*.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
**Example:**  
Device> enable |
| **Step 2** configure terminal | Enters global configuration mode.  
**Example:**  
Device# configure terminal |
| **Step 3** aaa new-model | Enables AAA.  
**Example:**  
Device(config)# aaa new-model |
| **Step 4** aaa authentication login {default | list-name} method1 [method2...]| Creates a login authentication method list.  
**Example:**  
Device(config)# aaa authentication login default tacacs+ local |

- **Step 1**: Enter your password if prompted.
- **Step 2**: Example: `Device# configure terminal`
- **Step 3**: Examples: `Device(config)# aaa new-model`
- **Step 4**: Examples: `Device(config)# aaa authentication login default tacacs+ local`

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

- For `list-name`, specify a character string to name the list you are creating.

- For `method1...`, specify the actual method the authentication algorithm tries. The additional methods of authentication are
Purpose

Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>used only if the previous method returns an error, not if it fails.</td>
<td></td>
</tr>
</tbody>
</table>

Select one of these methods:

- **enable**—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the `enable password` global configuration command.

- **group tacacs+**—Uses TACACS+ authentication. Before you can use this authentication method, you must configure the TACACS+ server.

- **line**—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.

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

- **local-case**—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.

- **none**—Do not use any authentication for login.

**Step 5**

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

**Example:**

```
Device(config)# line 2 4
```

Enters line configuration mode, and configures the lines to which you want to apply the authentication list.

**Step 6**

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

**Example:**

```
Device(config-line)# login authentication default
```

Applies the authentication list to a line or set of lines.

- If you specify `default`, use the default list created with the `aaa authentication login` command.

- For `list-name`, specify the list created with the `aaa authentication login` command.
### 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.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

#### 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:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device(config-line)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device# show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring TACACS+

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Configure the switch for user TACACS+ authorization for all network-related service requests.</td>
</tr>
<tr>
<td><code>aaa authorization network tacacs+</code></td>
<td></td>
</tr>
<tr>
<td><em>Example:</em> Device(config)# <code>aaa authorization network tacacs+</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configure the switch for user TACACS+ authorization if the user has privileged EXEC access.</td>
</tr>
<tr>
<td><code>aaa authorization exec tacacs+</code></td>
<td></td>
</tr>
<tr>
<td><em>Example:</em> Device(config)# <code>aaa authorization exec tacacs+</code></td>
<td>Configures the switch for user TACACS+ authorization if the user has privileged EXEC access. The <code>exec</code> keyword might return user profile information (such as <code>autocommand</code> information).</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><em>Example:</em> Device(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td><em>Example:</em> Device# <code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td><em>Example:</em> Device# <code>copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

### Starting TACACS+ Accounting

Follow these steps to start TACACS+ Accounting:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td><em>Example:</em> Device&gt; <code>enable</code></td>
<td></td>
</tr>
</tbody>
</table>

---

Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)
### Configuring TACACS+

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2** configure terminal  
Example:  
Device# configure terminal | Enters global configuration mode. |
| **Step 3** aaa accounting network start-stop tacacs+  
Example:  
Device(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:  
Device(config)# aaa accounting exec start-stop tacacs+ | 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. |
| **Step 5** end  
Example:  
Device(config)# end | Returns to privileged EXEC mode. |
| **Step 6** show running-config  
Example:  
Device# show running-config | Verifies your entries. |
| **Step 7** copy running-config startup-config  
Example:  
Device# 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.
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 24: Commands for Displaying TACACS+ Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show tacacs</code></td>
<td>Displays TACACS+ server statistics.</td>
</tr>
</tbody>
</table>

Additional References For Switch Access with TACACS+

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA configuration</td>
<td>Configuring Local Authentication and Authorization</td>
</tr>
</tbody>
</table>

**MIBs**

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

**Technical Assistance**

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

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 25: Feature Information for TACACS+

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS+</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through AAA and can be enabled only through AAA commands.</td>
</tr>
</tbody>
</table>
Configuring RADIUS

Prerequisites for Configuring RADIUS

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

General:

- RADIUS and Authentication, Authorization, and Accounting (AAA) must be enabled to use any of the configuration commands in this chapter.

- RADIUS is facilitated through AAA and can be enabled only through AAA commands.

- Use the `aaanew-model` global configuration command to enable AAA.

- Use the `aaa authentication` global configuration command to define method lists for RADIUS authentication.

- Use `line` and `interface` commands to enable the defined method lists to be used.

- At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.

- You should have access to and should configure a RADIUS server before configuring RADIUS features on your Device.

- 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.
For RADIUS operation:

- Users must first successfully complete RADIUS authentication before proceeding to RADIUS authorization, if it is enabled.

Restrictions for Configuring RADIUS

This topic covers restrictions for controlling Device 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.

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.

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 validates users and to grant access to network resources.
• Networks already using RADIUS. You can add a Cisco Device 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 10: Transitioning from RADIUS to TACACS+ Services

RADIUS Operation

When a user attempts to log in and authenticate to a Device 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:
RADIUS Change of Authorization

The RADIUS Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. When a policy changes for a user or user group in AAA, administrators can send RADIUS CoA packets from the AAA server such as a Cisco Secure Access Control Server (ACS) to reinitialize authentication and apply the new policy. This section provides an overview of the RADIUS interface including available primitives and how they are used during a CoA.

- Change-of-Authorization Requests
- CoA Request Response Code
- CoA Request Commands
- Session Reauthentication
- Stacking Guidelines for Session Termination

A standard RADIUS interface is typically used in a pulled model where the request originates from a network attached device and the response come from the queried servers. Catalyst support the RADIUS CoA extensions defined in RFC 5176 that are typically used in a pushed model and allow for the dynamic reconfiguring of sessions from external AAA or policy servers.

The supports these per-session CoA requests:

- Session reauthentication
- Session termination
- Session termination with port shutdown
- Session termination with port bounce

This feature is integrated with Cisco Secure Access Control Server (ACS) 5.1.

The RADIUS interface is enabled by default on Catalyst. However, some basic configuration is required for the following attributes:

- Security and Password—refer to the “Preventing Unauthorized Access to Your Switch” section in this guide.
- Accounting—refer to the “Starting RADIUS Accounting” section in the Configuring Switch-Based Authentication chapter in this guide.

Cisco IOS software supports the RADIUS CoA extensions defined in RFC 5176 that are typically used in a push model to allow the dynamic reconfiguring of sessions from external AAA or policy servers. Per-session CoA requests are supported for session identification, session termination, host reauthentication, port shutdown, and port bounce. This model comprises one request (CoA-Request) and two possible response codes:

- CoA acknowledgement (ACK) [CoA-ACK]
- CoA nonacknowledgement (NAK) [CoA-NAK]
The request is initiated from a CoA client (typically a AAA or policy server) and directed to the device that acts as a listener.

The table below shows the RADIUS CoA commands and vendor-specific attributes (VSAs) supported by Identity-Based Networking Services. All CoA commands must include the session identifier between the device and the CoA client.

**Table 26: RADIUS CoA Commands Supported by Identity-Based Networking Services**

<table>
<thead>
<tr>
<th>CoA Command</th>
<th>Cisco VSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate service</td>
<td>Cisco:Avpair=&quot;subscriber:command=activate-service&quot;</td>
</tr>
<tr>
<td></td>
<td>Cisco:Avpair=&quot;subscriber:service-name=&lt;service-name&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td>Cisco:Avpair=&quot;subscriber:precedence=&lt;precedence-number&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td>Cisco:Avpair=&quot;subscriber:activation-mode=replace-all&quot;</td>
</tr>
<tr>
<td>Deactivate service</td>
<td>Cisco:Avpair=&quot;subscriber:command=deactivate-service&quot;</td>
</tr>
<tr>
<td></td>
<td>Cisco:Avpair=&quot;subscriber:service-name=&lt;service-name&gt;&quot;</td>
</tr>
<tr>
<td>Bounce host port</td>
<td>Cisco:Avpair=&quot;subscriber:command=bounce-host-port&quot;</td>
</tr>
<tr>
<td>Disable host port</td>
<td>Cisco:Avpair=&quot;subscriber:command=disable-host-port&quot;</td>
</tr>
<tr>
<td>Session query</td>
<td>Cisco:Avpair=&quot;subscriber:command=session-query&quot;</td>
</tr>
<tr>
<td>Session reauthenticate</td>
<td>Cisco:Avpair=&quot;subscriber:command=reauthenticate&quot;</td>
</tr>
<tr>
<td></td>
<td>Cisco:Avpair=&quot;subscriber:reauthenticate-type=last&quot; or</td>
</tr>
<tr>
<td></td>
<td>Cisco:Avpair=&quot;subscriber:reauthenticate-type=rerun&quot;</td>
</tr>
<tr>
<td>Session terminate</td>
<td>This is a standard disconnect request and does not require a VSA.</td>
</tr>
<tr>
<td>Interface template</td>
<td>Cisco:AVpair=&quot;interface-template-name=&lt;interfacetemplate&gt;&quot;</td>
</tr>
</tbody>
</table>

**Change-of-Authorization Requests**

Change of Authorization (CoA) requests, as described in RFC 5176, are used in a push model to allow for session identification, host reauthentication, and session termination. The model is comprised of one request (CoA-Request) and two possible response codes:

- CoA acknowledgment (ACK) [CoA-ACK]
- CoA non-acknowledgment (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a RADIUS or policy server) and directed to the switch that acts as a listener.

**RFC 5176 Compliance**

The Disconnect Request message, which is also referred to as Packet of Disconnect (POD), is supported by the switch for session termination.
This table shows the IETF attributes are supported for this feature.

**Table 27: Supported IETF Attributes**

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>Attribute Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>State</td>
</tr>
<tr>
<td>31</td>
<td>Calling-Station-ID</td>
</tr>
<tr>
<td>44</td>
<td>Acct-Session-ID</td>
</tr>
<tr>
<td>80</td>
<td>Message-Authenticator</td>
</tr>
<tr>
<td>101</td>
<td>Error-Cause</td>
</tr>
</tbody>
</table>

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

**Table 28: Error-Cause Values**

<table>
<thead>
<tr>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Residual Session Context Removed</td>
</tr>
<tr>
<td>202</td>
<td>Invalid EAP Packet (Ignored)</td>
</tr>
<tr>
<td>401</td>
<td>Unsupported Attribute</td>
</tr>
<tr>
<td>402</td>
<td>Missing Attribute</td>
</tr>
<tr>
<td>403</td>
<td>NAS Identification Mismatch</td>
</tr>
<tr>
<td>404</td>
<td>Invalid Request</td>
</tr>
<tr>
<td>405</td>
<td>Unsupported Service</td>
</tr>
<tr>
<td>406</td>
<td>Unsupported Extension</td>
</tr>
<tr>
<td>407</td>
<td>Invalid Attribute Value</td>
</tr>
<tr>
<td>501</td>
<td>Administratively Prohibited</td>
</tr>
<tr>
<td>502</td>
<td>Request Not Routable (Proxy)</td>
</tr>
<tr>
<td>503</td>
<td>Session Context Not Found</td>
</tr>
<tr>
<td>504</td>
<td>Session Context Not Removable</td>
</tr>
<tr>
<td>505</td>
<td>Other Proxy Processing Error</td>
</tr>
<tr>
<td>506</td>
<td>Resources Unavailable</td>
</tr>
<tr>
<td>507</td>
<td>Request Initiated</td>
</tr>
<tr>
<td>508</td>
<td>Multiple Session Selection Unsupported</td>
</tr>
</tbody>
</table>
CoA Request Response Code

The CoA Request response code can be used to convey a command to the switch. The packet format for a CoA Request Response code as defined in RFC 5176 consists of the following fields: Code, Identifier, Length, Authenticator, and Attributes in the Type:Length:Value (TLV) format. The Attributes field is used to carry Cisco vendor-specific attributes (VSAs).

Session Identification

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

- Acct-Session-Id (IETF attribute #44)
- Audit-Session-Id (Cisco VSA)
- Calling-Station-Id (IETF attribute #31 which contains the host MAC address)
- IPv6 Attributes, which can be one of the following:
  - Framed-I Pv6-Prefix (IETF attribute #97) and Framed-Interface-Id (IETF attribute #96), which together create a full IPv6 address per RFC 3162
  - Framed-I Pv6-Address
- Plain IP Address (IETF attribute #8)

Unless all session identification attributes included in the CoA message match the session, the switch returns a Disconnect-NAK or CoA-NAK with the “Invalid Attribute Value” error-code attribute.

If more than one session identification attribute is included in the message, all the attributes must match the session or the switch returns a Disconnect- negative acknowledgment (NAK) or CoA-NAK with the error code “Invalid Attribute Value.”

The packet format for a CoA Request code as defined in RFC 5176 consists of the fields: Code, Identifier, Length, Authenticator, and Attributes in Type:Length:Value (TLV) format.

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----------------------------------------------+
| Code | Identifier | Length |
+-----------------------------------------------+
| | Authenticator |
+-----------------------------------------------+
| Attributes ...
+-----------------------------------------------+
```

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

For CoA requests targeted at a particular enforcement policy, the device returns a CoA-NAK with the error code “Invalid Attribute Value” if any of the above session identification attributes are included in the message.
CoA ACK Response Code

If the authorization state is changed successfully, a positive acknowledgment (ACK) is sent. The attributes returned within CoA ACK will vary based on the CoA Request and are discussed in individual CoA Commands.

CoA NAK Response Code

A negative acknowledgment (NAK) indicates a failure to change the authorization state and can include attributes that indicate the reason for the failure. Use `show` commands to verify a successful CoA.

CoA Request Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Cisco VSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reauthenticate host</td>
<td><code>Cisco:Avpair=&quot;subscriber:command=reauthenticate&quot;</code></td>
</tr>
<tr>
<td>Terminate session</td>
<td>This is a standard disconnect request that does not require a VSA.</td>
</tr>
<tr>
<td>Bounce host port</td>
<td><code>Cisco:Avpair=&quot;subscriber:command=bounce-host-port&quot;</code></td>
</tr>
<tr>
<td>Disable host port</td>
<td><code>Cisco:Avpair=&quot;subscriber:command=disable-host-port&quot;</code></td>
</tr>
</tbody>
</table>

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

Session Reauthentication

The AAA server typically generates a session reauthentication request when a host with an unknown identity or posture joins the network and is associated with a restricted access authorization profile (such as a guest VLAN). A reauthentication request allows the host to be placed in the appropriate authorization group when its credentials are known.

To initiate session authentication, the AAA server sends a standard CoA-Request message which contains a Cisco VSA in this form: `Cisco:Avpair="subscriber:command=reauthenticate"` and one or more session identification attributes.

The current session state determines the switch response to the message. If the session is currently authenticated by IEEE 802.1x, the switch responds by sending an EAPoL (Extensible Authentication Protocol over Lan) -RequestId message to the server.

If the session is currently authenticated by MAC authentication bypass (MAB), the switch sends an access-request to the server, passing the same identity attributes used for the initial successful authentication.

If session authentication is in progress when the switch receives the command, the switch terminates the process, and restarts the authentication sequence, starting with the method configured to be attempted first.

If the session is not yet authorized, or is authorized via guest VLAN, or critical VLAN, or similar policies, the reauthentication message restarts the access control methods, beginning with the method configured to be attempted first. The current authorization of the session is maintained until the reauthentication leads to a different authorization result.

Session Reauthentication in a Switch Stack

When a switch stack receives a session reauthentication message:
• It checkpoints the need for a re-authentication before returning an acknowledgment (ACK).

• It initiates reauthentication for the appropriate session.

• If authentication completes with either success or failure, the signal that triggered the reauthentication is removed from the stack member.

• If the stack master fails before authentication completes, reauthentication is initiated after stack master switch-over based on the original command (which is subsequently removed).

• If the stack master fails before sending an ACK, the new stack master treats the re-transmitted command as a new command.

Session Termination

There are three types of CoA requests that can trigger session termination. A CoA Disconnect-Request terminates the session, without disabling the host port. This command causes re-initialization of the authenticator state machine for the specified host, but does not restrict that host access to the network.

To restrict a host’s access to the network, use a CoA Request with the Cisco:Avpair="subscriber:command=disable-host-port" VSA. This command is useful when a host is known to be causing problems on the network, and you need to immediately block network access for the host. When you want to restore network access on the port, re-enable it using a non-RADIUS mechanism.

When a device with no supplicant, such as a printer, needs to acquire a new IP address (for example, after a VLAN change), terminate the session on the host port with port-bounce (temporarily disable and then re-enable the port).

CoA Disconnect-Request

This command is a standard Disconnect-Request. If the session cannot be located, the switch returns a Disconnect-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the switch terminates the session. After the session has been completely removed, the switch returns a Disconnect-ACK.

If the switch fails-over to a standby switch before returning a Disconnect-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the session is not found following re-sending, a Disconnect-ACK is sent with the “Session Context Not Found” error-code attribute.

CoA Request: Disable Host Port

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. To restore network access on the port, re-enable it using a non-RADIUS mechanism. This command is carried in a standard CoA-Request message that has this new vendor-specific attribute (VSA):

Cisco:Avpair="subscriber:command=disable-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the “Session Identification” section. If the session cannot be located, the switch returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the switch disables the hosting port and returns a CoA-ACK message.

If the switch fails before returning a CoA-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the switch fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is restarted on the new active switch.
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.

**CoA Request: Bounce-Port**

A RADIUS server CoA bounce port sent from a RADIUS server can cause a link flap on an authentication port, which triggers DHCP renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer) that does not have a mechanism to detect a change on this authentication port. The CoA bounce port is carried in a standard CoA-Request message that contains the following VSA:

Cisco:Avpair="subscriber:command=bounce-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes. If the session cannot be located, the switch returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the switch disables the hosting port for a period of 10 seconds, re-enables it (port-bounce), and returns a CoA-ACK.

If the switch fails before returning a CoA-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the switch fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is re-started on the new active switch.

**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.

**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.

**AAA Server Groups**

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

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If you configure two different host entries on the same RADIUS server for the same service, (for example, accounting), the second configured host entry acts as a fail-over backup to the first one. If the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order in which they are configured.)

**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.

**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.

**Vendor-Specific RADIUS Attributes**

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the switch and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco’s vendor-ID is 9, and the supported option has vendor-type 1, which is named `cisco-avpair`. The value is a string with this format:

```
protocol : attribute sep value *
```

*Protocol* is a value of the Cisco protocol attribute for a particular type of authorization. *Attribute* and *value* are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and *sep* is = for mandatory attributes and is * for optional attributes. The full set of features available for TACACS+ authorization can then be used for RADIUS.

For example, the following AV pair causes Cisco’s “multiple named IP address pools” feature to be activated during IP authorization (during PPP’s Internet Protocol Control Protocol (IPCP) address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

If you insert an “*”, the AV pair “ip:addr-pool=first” becomes optional. Note that any AV pair can be made optional:

```
cisco-avpair= "ip:addr-pool*first"
```

The following example shows how to cause a user logging in from a network access server to have immediate access to EXEC commands:

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, see RFC 2138, “Remote Authentication Dial-In User Service (RADIUS).”

Attribute 26 contains the following three elements:

- Type
- Length
- String (also known as data)
  - Vendor-Id
  - Vendor-Type
  - Vendor-Length
  - Vendor-Data

The figure below shows the packet format for a VSA encapsulated “behind” attribute 26.
It is up to the vendor to specify the format of their VSA. The Attribute-Specific field (also known as Vendor-Data) is dependent on the vendor's definition of that attribute.

The table below describes significant fields listed in the Vendor-Specific RADIUS IETF Attributes table (second table below), which lists supported vendor-specific RADIUS attributes (IETF attribute 26).

### Table 30: Vendor-Specific Attributes Table Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>All attributes listed in the following table are extensions of IETF attribute 26.</td>
</tr>
<tr>
<td>Vendor-Specific Command Codes</td>
<td>A defined code used to identify a particular vendor. Code 9 defines Cisco VSAs, 311 defines Microsoft VSAs, and 529 defines Ascend VSAs.</td>
</tr>
<tr>
<td>Sub-Type Number</td>
<td>The attribute ID number. This number is much like the ID numbers of IETF attributes, except it is a &quot;second layer&quot; ID number encapsulated behind attribute 26.</td>
</tr>
<tr>
<td>Attribute</td>
<td>The ASCII string name of the attribute.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the attribute.</td>
</tr>
</tbody>
</table>

### Table 31: Vendor-Specific RADIUS IETF Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>311</td>
<td>1</td>
<td>MSCHAP-Response</td>
<td>Contains the response value provided by a PPP MS-CHAP user in response to the challenge. It is only used in Access-Request packets. This attribute is identical to the PPP CHAP Identifier. (RFC 2548)</td>
</tr>
</tbody>
</table>
### Vendor-Specific RADIUS Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>311</td>
<td>11</td>
<td>MSCHAP-Challenge</td>
<td>Contains the challenge sent by a network access server to an MS-CHAP user. It can be used in both Access-Request and Access-Challenge packets. (RFC 2548)</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>12tp-cm-local-window-size</td>
<td>Specifies the maximum receive window size for L2TP control messages. This value is advertised to the peer during tunnel establishment.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>12tp-drop-out-of-order</td>
<td>Respects sequence numbers on data packets by dropping those that are received out of order. This does not ensure that sequence numbers will be sent on data packets, just how to handle them if they are received.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>12tp-hello-interval</td>
<td>Specifies the number of seconds for the hello keepalive interval. Hello packets are sent when no data has been sent on a tunnel for the number of seconds configured here.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>12tp-hidden-avp</td>
<td>When enabled, sensitive AVPs in L2TP control messages are scrambled or hidden.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>12tp-nosession-timeout</td>
<td>Specifies the number of seconds that a tunnel will stay active with no sessions before timing out and shutting down.</td>
</tr>
</tbody>
</table>
## Vendor-Specific RADIUS Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>tunnel-tos-reflect</td>
<td>Copies the IP ToS field from the IP header of each payload packet to the IP header of the tunnel packet for packets entering the tunnel at the LNS.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>l2tp-tunnel-authen</td>
<td>If this attribute is set, it performs L2TP tunnel authentication.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>l2tp-tunnel-password</td>
<td>Shared secret used for L2TP tunnel authentication and AVP hiding.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>l2tp-udp-checksum</td>
<td>This is an authorization attribute and defines whether L2TP should perform UDP checksums for data packets. Valid values are “yes” and “no.” The default is no.</td>
</tr>
</tbody>
</table>

### Store and Forward Fax Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>3</td>
<td>Fax-Account-Id-Origin</td>
<td>Indicates the account ID origin as defined by system administrator for the \texttt{mnoip aaa receive-id} or the \texttt{mnoip aaa send-id} commands.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>4</td>
<td>Fax-Msg-Id=</td>
<td>Indicates a unique fax message identification number assigned by Store and Forward Fax.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>5</td>
<td>Fax-Pages</td>
<td>Indicates the number of pages transmitted or received during this fax session. This page count includes cover pages.</td>
</tr>
<tr>
<td>Number</td>
<td>Vendor-Specific Company Code</td>
<td>Sub-Type Number</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------</td>
<td>-----------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>6</td>
<td>Fax-Coverpage-Flag</td>
<td>Indicates whether or not a cover page was generated by the off-ramp gateway for this fax session. True indicates that a cover page was generated; false means that a cover page was not generated.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>7</td>
<td>Fax-Modem-Time</td>
<td>Indicates the amount of time in seconds the modem sent fax data (x) and the amount of time in seconds of the total fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds, and the total fax session took 15 seconds.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>8</td>
<td>Fax-Connect-Speed</td>
<td>Indicates the modems speed at which this fax-mail was initially transmitted or received. Possible values are 1200, 4800, 9600, and 14400.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>9</td>
<td>Fax-Recipient-Count</td>
<td>Indicates the number of recipients for this fax transmission. Until e-mail servers support Session mode, the number should be 1.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>10</td>
<td>Fax-Process-Abort-Flag</td>
<td>Indicates that the fax session was aborted or successful. True means that the session was aborted; false means that the session was successful.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>11</td>
<td>Fax-Dsn-Address</td>
<td>Indicates the address to which DSNs will be sent.</td>
</tr>
<tr>
<td>Number</td>
<td>Vendor-Specific Company Code</td>
<td>Sub-Type Number</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------</td>
<td>-----------------</td>
<td>----------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>12</td>
<td>Fax-Dsn-Flag</td>
<td>Indicates whether or not DSN has been enabled. True indicates that DSN has been enabled; false means that DSN has not been enabled.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>13</td>
<td>Fax-Mdn-Address</td>
<td>Indicates the address to which MDNs will be sent.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>14</td>
<td>Fax-Mdn-Flag</td>
<td>Indicates whether or not message delivery notification (MDN) has been enabled. True indicates that MDN had been enabled; false means that MDN had not been enabled.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>15</td>
<td>Fax-Auth-Status</td>
<td>Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>16</td>
<td>Email-Server-Address</td>
<td>Indicates the IP address of the e-mail server handling the on-ramp fax-mail message.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>17</td>
<td>Email-Server-Ack-Flag</td>
<td>Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>18</td>
<td>Gateway-Id</td>
<td>Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>19</td>
<td>Call-Type</td>
<td>Describes the type of fax activity: fax receive or fax send.</td>
</tr>
<tr>
<td>Number</td>
<td>Vendor-Specific Company Code</td>
<td>Sub-Type Number</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------</td>
<td>-----------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>20</td>
<td>Port-Used</td>
<td>Indicates the slot/port number of the Cisco AS5300 used to either transmit or receive this fax-mail.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>21</td>
<td>Abort-Cause</td>
<td>If the fax session aborts, indicates the system component that signaled the abort. Examples of system components that could trigger an abort are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server.</td>
</tr>
</tbody>
</table>

**H323 Attributes**

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>23</td>
<td>Remote-Gateway-ID (h323-remote-address)</td>
<td>Indicates the IP address of the remote gateway.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>24</td>
<td>Connection-ID (h323-conf-id)</td>
<td>Identifies the conference ID.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>25</td>
<td>Setup-Time (h323-setup-time)</td>
<td>Indicates the setup time for this connection in Coordinated Universal Time (UTC) formerly known as Greenwich Mean Time (GMT) and Zulu time.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>26</td>
<td>Call-Origin (h323-call-origin)</td>
<td>Indicates the origin of the call relative to the gateway. Possible values are originating and terminating (answer).</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>27</td>
<td>Call-Type (h323-call-type)</td>
<td>Indicates call leg type. Possible values are telephony and VoIP.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>28</td>
<td>Connect-Time (h323-connect-time)</td>
<td>Indicates the connection time for this call leg in UTC.</td>
</tr>
<tr>
<td>Number</td>
<td>Vendor-Specific Company Code</td>
<td>Sub-Type Number</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------</td>
<td>-----------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>29</td>
<td>Disconnect-Time (h323-disconnect-time)</td>
<td>Indicates the time this call leg was disconnected in UTC.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>30</td>
<td>Disconnect-Cause (h323-disconnect-cause)</td>
<td>Specifies the reason a connection was taken offline per Q.931 specification.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>31</td>
<td>Voice-Quality (h323-voice-quality)</td>
<td>Specifies the impairment factor (ICPIF) affecting voice quality for a call.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>33</td>
<td>Gateway-ID (h323-gw-id)</td>
<td>Indicates the name of the underlying gateway.</td>
</tr>
</tbody>
</table>

**Large Scale Dialout Attributes**

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>callback-dialstring</td>
<td>Defines a dialing string to be used for callback.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>data-service</td>
<td>No description available.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>dial-number</td>
<td>Defines the number to dial.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>force-56</td>
<td>Determines whether the network access server uses only the 56 K portion of a channel, even when all 64 K appear to be available.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>map-class</td>
<td>Allows the user profile to reference information configured in a map class of the same name on the network access server that dials out.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>send-auth</td>
<td>Defines the protocol to use (PAP or CHAP) for username-password authentication following CLID authentication.</td>
</tr>
</tbody>
</table>
### Vendor-Specific RADIUS Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| 26     | 9                           | 1               | send-name | PPP name authentication. To apply for PAP, do not configure the `ppp pap sent-name password` command on the interface. For PAP, “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication. For CHAP, “preauth:send-name” will be used not only for outbound authentication, but also for inbound authentication. For a CHAP inbound case, the NAS will use the name defined in “preauth:send-name” in the challenge packet to the caller box.

**Note**  The send-name attribute has changed over time: Initially, it performed the functions now provided by both the send-name and remote-name attributes. Because the remote-name attribute has been added, the send-name attribute is restricted to its current behavior. |
### Vendor-Specific RADIUS Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>send-secret</td>
<td>PPP password authentication. The vendor-specific attributes (VSAs) “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication. For a CHAP outbound case, both “preauth:send-name” and “preauth:send-secret” will be used in the response packet.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>remote-name</td>
<td>Provides the name of the remote host for use in large-scale dial-out. Dialer checks that the large-scale dial-out remote name matches the authenticated name, to protect against accidental user RADIUS misconfiguration. (For example, dialing a valid phone number but connecting to the wrong device.)</td>
</tr>
</tbody>
</table>

**Miscellaneous Attributes**
Cisco-NAS-Port

Specifies additional vendor specific attribute (VSA) information for NAS-Port accounting. To specify additional NAS-Port information in the form an Attribute-Value Pair (AVPair) string, use the `radius-server vsa send` global configuration command.

**Note** This VSA is typically used in Accounting, but may also be used in Authentication (Access-Request) packets.

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>2</td>
<td>Cisco-NAS-Port</td>
<td>Specifies additional vendor specific attribute (VSA) information for NAS-Port accounting. To specify additional NAS-Port information in the form an Attribute-Value Pair (AVPair) string, use the <code>radius-server vsa send</code> global configuration command.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>min-links</td>
<td>Sets the minimum number of links for MLP.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td><code>proxyacl#&lt;n&gt;</code></td>
<td>Allows users to configure the downloadable user profiles (dynamic ACLs) by using the authentication proxy feature so that users can have the configured authorization to permit traffic going through the configured interfaces.</td>
</tr>
</tbody>
</table>
### Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the switch and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the switch. You specify the RADIUS host and secret text string by using the `radius server` global configuration commands.

### How to Configure RADIUS

#### Identifying the RADIUS Server Host

To apply these settings globally to all RADIUS servers communicating with the Device, use the three unique global configuration commands: `radius-server timeout`, `radius-server retransmit`, and `key string`.

You can configure the Device 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 Device and the key string to be shared by both the server and the Device. For more information, see the RADIUS server documentation.

Follow these steps to configure per-server RADIUS server communication.

---

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>spi</td>
<td>Carries the authentication information needed by the home agent to authenticate a mobile node during registration. The information is in the same syntax as the <code>ip mobile secure host &lt;addr&gt;</code> configuration command. Basically it contains the rest of the configuration command that follows that string, verbatim. It provides the Security Parameter Index (SPI), key, authentication algorithm, authentication mode, and replay protection timestamp range.</td>
</tr>
</tbody>
</table>
Before you begin

If you configure both global and per-server functions (timeout, retransmission, and key commands) on the device, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these settings on all RADIUS servers, see Related Topics below.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> radius server server name</td>
<td>(Optional) Specifies the RADIUS server</td>
</tr>
<tr>
<td>Example:</td>
<td>parameters.</td>
</tr>
<tr>
<td>Device(config)# radius server rsim</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> address {ipv4</td>
<td>ipv6}ip address { auth-port port number</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-radius-server)# address ipv4 124.2.2.12 auth-port 1612</td>
<td>(Optional) For key string, specify the authentication and encryption key used between the Device and the RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td><strong>Step 5</strong> key string</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-radius-server)# key radi123</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---

**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` 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.

---

**Step 6** `retransmit value`

*Example:*

Device(config-radius-server)# `retransmit 10`

*(Optional) Specifies the number of times a RADIUS request is resent when the server is not responding or responding slowly. The range is 1 to 100. This setting overrides the `radius-server retransmit` global configuration command setting.*

---

**Step 7** `timeout seconds`

*Example:*

Device(config-radius-server)# `timeout 60`

*(Optional) Specifies the time interval that the Device waits for the RADIUS server to reply before sending a request again. The range is 1 to 1000. This setting overrides the `radius-server timeout` global configuration command setting.*

---

**Step 8** `exit`

*Example:*

Device(config-server-tacacs)# `exit`

*Exits the RADIUS server mode and enters the global configuration mode.*

---

**Step 9** `end`

*Example:*

Device(config)# `end`

*Returns to privileged EXEC mode.*

---

**Step 10** `show running-config`

*Example:*

Device# `show running-config`

*Verifies your entries.*

---

**Step 11** `copy running-config startup-config`

*Example:*

Device# `copy running-config`

*(Optional) Saves your entries in the configuration file.*
Configuring RADIUS Login Authentication

Follow these steps to configure RADIUS login authentication:

Before you begin

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>aaa new-model</code></td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# aaa new-model</code></td>
<td></td>
</tr>
<tr>
<td>`aaa authentication login {default</td>
<td>list-name} method1 [method2...]`</td>
</tr>
<tr>
<td>Example:</td>
<td>• To create a default list that is used when a named list is not specified in the <code>login authentication</code> command, use the <code>default</code> keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports.</td>
</tr>
<tr>
<td><code>Device(config)# aaa authentication login default local</code></td>
<td>• For <code>list-name</code>, specify a character string to name the list you are creating.</td>
</tr>
<tr>
<td></td>
<td>• For <code>method1...</code>, specify the actual method the authentication algorithm tries. The additional methods of authentication are</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>used only if the previous method returns an error, not if it fails.</td>
</tr>
</tbody>
</table>

Select one of these methods:

- **enable** — Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the `enable password` global configuration command.

- **group radius** — Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server.

- **line** — 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.

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

- **local-case** — 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.

- **none** — Do not use any authentication for login.

---

### Step 5

**Command:**

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

**Example:**

```
Device(config)# line 1 4
```

Enters line configuration mode, and configure the lines to which you want to apply the authentication list.

---

### Step 6

**Command:**

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

**Example:**

Applies the authentication list to a line or set of lines.
### 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:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; <strong>enable</strong></td>
<td>Enters your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# <strong>configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>radius server <em>name</em></td>
<td>Specifies the name of the RADIUS server configuration for Protected Access Credential (PAC) provisioning and enters RADIUS server configuration mode. The device also supports RADIUS for IPv6.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# radius server ISE</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>address {ipv4</td>
<td>ipv6} {ip-address</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>key <em>string</em></td>
<td>Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-radius-server)# key cisco123</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>end</td>
<td>Exits RADIUS server configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-radius-server)# end</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# show running-config</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# copy running-config startup-config</td>
</tr>
</tbody>
</table>
Configuring RADIUS Authorization for User Privileged Access and Network Services

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

Follow these steps to configure RADIUS authorization for user privileged access and network services:

### Procedure

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

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

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>aaa authorization network radius</td>
<td>Configures the device for user RADIUS authorization for all network-related service requests.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# aaa authorization network radius</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>aaa authorization exec radius</td>
<td>Configures the device for user RADIUS authorization if the user has privileged EXEC access.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>The exec keyword might return user profile information (such as autocmd information).</td>
</tr>
<tr>
<td>Device(config)# aaa authorization exec radius</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Device# show running-config</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 7**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**Example:**

Device# copy running-config startup-config

---

**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.

---

**Starting RADIUS Accounting**

Follow these steps to start RADIUS accounting:

**Procedure**

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

**Step 2**

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

**Step 3**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting network start-stop radius</td>
<td>Enables RADIUS accounting for all network-related service requests.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# aaa accounting network start-stop radius</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Settings for All RADIUS Servers

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> radius-server key <em>string</em></td>
<td>Specifies the shared secret text string used between the switch and all RADIUS servers.</td>
</tr>
</tbody>
</table>

---

### Configuring Settings for All RADIUS Servers

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

**Purpose**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>aaa accounting exec start-stop radius</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

---

**Example:**

- **Step 4**
  ```
  Device(config)# aaa accounting exec start-stop radius
  ```

- **Step 5**
  ```
  Device(config)# end
  ```

- **Step 6**
  ```
  Device# show running-config
  ```

- **Step 7**
  ```
  Device# copy running-config startup-config
  ```
### Configuring Settings for All RADIUS Servers

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config)# radius-server key your_server_key</code></td>
<td><strong>Note</strong> The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</td>
</tr>
<tr>
<td><code>Device(config)# key your_server_key</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

**radius-server retransmit** *retries*

*Example:*

```
Device(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** *seconds*

*Example:*

```
Device(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.

**Step 5**

**radius-server deadtime** *minutes*

*Example:*

```
Device(config)# radius-server deadtime 0
```

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:*

```
Device(config)# end
```

Returns to privileged EXEC mode.

**Step 7**

**show running-config**

*Example:*

```
Device# show running-config
```

Verifies your entries.

**Step 8**

**copy running-config startup-config**

*Example:*

```
Device# copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.
# Configuring the Device to Use Vendor-Specific RADIUS Attributes

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

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable            | Enables privileged EXEC mode.  
  Example:  
  Device> enable |
| **Step 2** | configure terminal | Enters global configuration mode. |
| **Step 3** | radius-server vsa send [accounting | Enables the device to recognize and use VSAs as defined by RADIUS IETF attribute 26.  
  authentication]  
  Example:  
  Device(config)# radius-server vsa send accounting |
| **Step 4** | end               | Returns to privileged EXEC mode.  
  Example:  
  Device(config)# end |
| **Step 5** | show running-config | Verifies your entries.  
  Example:  
  Device# show running-config |
| **Step 6** | copy running-config startup-config | (Optional) Saves your entries in the configuration file.  
  Example:  
  Device# copy running-config startup-config |
Configuring the Device for Vendor-Proprietary RADIUS Server Communication

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  *enable*  
  **Example:**
  Device> enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Step 2**
  *configure terminal*  
  **Example:**
  Device# configure terminal | Enters global configuration mode. |
| **Step 3**
  *radius server server name*  
  **Example:**
  Device(config)# radius server rsim | Specifies the RADIUS server. |
| **Step 4**
  *address { ipv4 | ipv6 } ip address*  
  **Example:**
  Device(config-radius-server)# address  
  ipv4 172.24.25.10 | (Optional) Specifies the IP address of the RADIUS server. |
| **Step 5**
  *non-standard*  
  **Example:**
  Device(config-radius-server)# non-standard | Identifies that the RADIUS server using a vendor-proprietary implementation of RADIUS. |
| **Step 6**
  *key string*  
  **Example:**
  Device(config-radius-server)# key rad123 | Specifies the shared secret text string used between the device and the vendor-proprietary RADIUS server. The device and the RADIUS server use this text string to encrypt passwords and exchange responses. |
## Configuring CoA on the Device

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

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>3</td>
<td>aaa new-model</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# aaa new-model</td>
</tr>
<tr>
<td>4</td>
<td>aaa server radius dynamic-author</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# aaa server radius dynamic-author</td>
</tr>
<tr>
<td>5</td>
<td>client {ip-address</td>
</tr>
<tr>
<td>6</td>
<td>server-key [0</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-sg-radius)# server-key your_server_key</td>
</tr>
<tr>
<td>7</td>
<td>port port-number</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-sg-radius)# port 25</td>
</tr>
<tr>
<td>8</td>
<td>auth-type {any</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-sg-radius)# auth-type any</td>
</tr>
<tr>
<td>9</td>
<td>ignore session-key</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-sg-radius)# ignore</td>
</tr>
<tr>
<td>10</td>
<td>ignore server-key</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
</tbody>
</table>
### Monitoring CoA Functionality

#### Table 32: Privileged EXEC show Commands

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>server-key</code></td>
<td>Displays AAA attributes of RADIUS commands.</td>
</tr>
<tr>
<td><code>authentication command bounce-port ignore</code></td>
<td>(Optional) Configures the device 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.</td>
</tr>
<tr>
<td><code>authentication command disable-port ignore</code></td>
<td>(Optional) Configures the device 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.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Table 33: Global Troubleshooting Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug radius</td>
<td>Displays information for troubleshooting RADIUS.</td>
</tr>
<tr>
<td>debug aaa coa</td>
<td>Displays information for troubleshooting CoA processing.</td>
</tr>
<tr>
<td>debug aaa pod</td>
<td>Displays information for troubleshooting POD packets.</td>
</tr>
<tr>
<td>debug aaa subsys</td>
<td>Displays information for troubleshooting POD packets.</td>
</tr>
<tr>
<td>debug cmdhd [detail</td>
<td>error</td>
</tr>
</tbody>
</table>

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

Feature Information for RADIUS

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 34: Feature Information for RADIUS

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>The Auto Identity feature provides a set of built-in policies at the global configuration and interface configuration modes. This feature is available only in the Class-Based Policy Language (CPL) control policy-equivalent new-style mode. The following commands was introduced or modified: source-template.</td>
</tr>
</tbody>
</table>
Configuring Kerberos

- Prerequisites for Controlling Switch Access with Kerberos, on page 173
- Information about Kerberos, on page 173
- How to Configure Kerberos, on page 177
- Monitoring the Kerberos Configuration, on page 177
- Additional References, on page 177
- Feature Information for Kerberos, on page 178

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.
This section describes how to enable and configure the Kerberos security system, which authenticates requests for network resources by using a trusted third party.

In the Kerberos configuration examples, the trusted third party can be any switch that supports Kerberos, that is configured as a network security server, and that can authenticate users by using the Kerberos protocol.

Kerberos Overview

Kerberos is a secret-key network authentication protocol, which was developed at the Massachusetts Institute of Technology (MIT). It uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication and authenticates requests for network resources. Kerberos uses the concept of a trusted third party to perform secure verification of users and services. This trusted third party is called the key distribution center (KDC).

Kerberos verifies that users are who they claim to be and the network services that they use are what the services claim to be. To do this, a KDC or trusted Kerberos server issues tickets to users. These tickets, which have a limited life span, are stored in user credential caches. The Kerberos server uses the tickets instead of user names and passwords to authenticate users and network services.

A Kerberos server can be any switch that is configured as a network security server and that can authenticate users by using the Kerberos protocol.

The Kerberos credential scheme uses a process called single logon. This process authenticates a user once and then allows secure authentication (without encrypting another password) wherever that user credential is accepted.

This software release supports Kerberos 5, which allows organizations that are already using Kerberos 5 to use the same Kerberos authentication database on the KDC that they are already using on their other network hosts (such as UNIX servers and PCs).

Kerberos supports these network services:

• Telnet
• rlogin
• rsh

This table lists the common Kerberos-related terms and definitions.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>A process by which a user or service identifies itself to another service. For example, a client can authenticate to a switch or a switch can authenticate to another switch.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authorization</td>
<td>A means by which the switch identifies what privileges the user has in a network or on the switch and what actions the user can perform.</td>
</tr>
<tr>
<td>Credential</td>
<td>A general term that refers to authentication tickets, such as TGTs and service credentials. Kerberos credentials verify the identity of a user or service. If a network service decides to trust the Kerberos server that issued a ticket, it can be used in place of re-entering a username and password. Credentials have a default life span of eight hours.</td>
</tr>
<tr>
<td>Instance</td>
<td>An authorization level label for Kerberos principals. Most Kerberos principals are of the form user@REALM (for example, <a href="mailto:smith@EXAMPLE.COM">smith@EXAMPLE.COM</a>). A Kerberos principal with a Kerberos instance has the form user/instance@REALM (for example, smith/admin@EXAMPLE.COM). The Kerberos instance can be used to specify the authorization level for the user if authentication is successful. The server of each network service might implement and enforce the authorization mappings of Kerberos instances but is not required to do so.</td>
</tr>
<tr>
<td>Note</td>
<td>The Kerberos principal and instance names must be in all lowercase characters.</td>
</tr>
<tr>
<td>Note</td>
<td>The Kerberos realm name must be in all uppercase characters.</td>
</tr>
<tr>
<td>KDC</td>
<td>Key distribution center that consists of a Kerberos server and database program that is running on a network host.</td>
</tr>
<tr>
<td>Kerberized</td>
<td>A term that describes applications and services that have been modified to support the Kerberos credential infrastructure.</td>
</tr>
<tr>
<td>Kerberos realm</td>
<td>A domain consisting of users, hosts, and network services that are registered to a Kerberos server. The Kerberos server is trusted to verify the identity of a user or network service to another user or network service.</td>
</tr>
<tr>
<td>Note</td>
<td>The Kerberos realm name must be in all uppercase characters.</td>
</tr>
<tr>
<td>Kerberos server</td>
<td>A daemon that is running on a network host. Users and network services register their identity with the Kerberos server. Network services query the Kerberos server to authenticate to other network services.</td>
</tr>
<tr>
<td>KEYTAB</td>
<td>A password that a network service shares with the KDC. In Kerberos 5 and later Kerberos versions, the network service authenticates an encrypted service credential by using the KEYTAB to decrypt it. In Kerberos versions earlier than Kerberos 5, KEYTAB is referred to as SRVTAB.</td>
</tr>
<tr>
<td>Principal</td>
<td>Also known as a Kerberos identity, this is who you are or what a service is according to the Kerberos server.</td>
</tr>
<tr>
<td>Note</td>
<td>The Kerberos principal name must be in all lowercase characters.</td>
</tr>
<tr>
<td>Service credential</td>
<td>A credential for a network service. When issued from the KDC, this credential is encrypted with the password shared by the network service and the KDC. The password is also shared with the user TGT.</td>
</tr>
</tbody>
</table>
**Term** | **Definition**
--- | ---
SRVTAB | A password that a network service shares with the KDC. In Kerberos 5 or later Kerberos versions, SRVTAB is referred to as KEYTAB.
TGT | 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.

---

**Kerberos Operation**

A Kerberos server can be a device 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 device as a Kerberos server, remote users must follow these steps:

**Authenticating to a Boundary Switch**

This section describes the first layer of security through which a remote user must pass. The user must first authenticate to the boundary switch. This process then occurs:

1. The user opens an un-Kerberized Telnet connection to the boundary switch.
2. The switch prompts the user for a username and password.
3. The switch requests a TGT from the KDC for this user.
4. The KDC sends an encrypted TGT that includes the user identity to the switch.
5. The switch attempts to decrypt the TGT by using the password that the user entered.
   - If the decryption is successful, the user is authenticated to the switch.
   - 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 an un-Kerberized Telnet session and authenticates to a boundary switch is inside the firewall, but the user must still authenticate directly to the KDC before getting access to the network services. The user must authenticate to the KDC because the TGT that the KDC issues is stored on the switch and cannot be used for additional authentication until the user logs on to the switch.

**Obtaining a TGT from a KDC**

This section describes the second layer of security through which a remote user must pass. The user must now authenticate to a KDC and obtain a TGT from the KDC to access network services.
For instructions about how to authenticate to a KDC, see the “Obtaining a TGT from a KDC” section in the “Security Server Protocols” chapter of the *Cisco IOS Security Configuration Guide, Release 12.4*.

**Authenticating to Network Services**

This section describes the third layer of security through which a remote user must pass. The user with a TGT must now authenticate to the network services in a Kerberos realm.

For instructions about how to authenticate to a network service, see the “Authenticating to Network Services” section in the “Security Server Protocols” chapter of the *Cisco IOS Security Configuration Guide, Release 12.4*.

**How to Configure Kerberos**

To set up a Kerberos-authenticated server-client system, follow these steps:

- Configure the KDC by using Kerberos commands.
- Configure the switch to use the Kerberos protocol.

**Monitoring the Kerberos Configuration**

To display the Kerberos configuration, use the following commands:

- `show running-config`
- `show kerberos creds`: Lists the credentials in a current user’s credentials cache.
- `clear kerberos creds`: Destroys all credentials in a current user’s credentials cache, including those forwarded.

**Additional References**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos Commands</td>
<td><em>Cisco IOS Security Command Reference</em></td>
</tr>
</tbody>
</table>

**Error Message Decoder**

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

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 36: Feature Information for Kerberos

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>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.</td>
</tr>
</tbody>
</table>
MACsec Encryption

• Restrictions for MACsec Encryption, on page 179
• Information about MACsec Encryption, on page 179
• How to Configure MACsec Encryption, on page 186
• Configuring Examples for MACsec Encryption, on page 202

Restrictions for MACsec Encryption

• MACsec Key Agreement (MKA) is not supported with high availability.

• MKA policy can only be applied to member of a port-channel. You cannot apply MKA policy to a port-channel.

• MACsec is not supported in SVL mode for Cisco TrustSec and MKA.

• MACsec is not supported with C9400-SUP-1XL-Y supervisor module. It is supported only with C9400-SUP-1 and C9400-SUP-1XL supervisor module.

• Promiscuous Private VLAN (P VLAN) ports are not supported.

• Delay protection and confidentiality offset of 50 is not supported on the supervisor ports.

• Only multihost mode is supported for MACsec MKA using EAP-TLS. Single host mode and Multi Domain Authentication (MDA) mode is not supported.

Information about MACsec Encryption

MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. Cisco Catalyst 9400 Series Switches support 802.1AE encryption with MACsec Key Agreement (MKA) on the line card ports for encryption between the switch and the host device. The switch also supports MACsec encryption for switch-to-switch (inter-network device) security using both Cisco TrustSec Network Device Admission Control (NDAC), Security Association Protocol (SAP) and MKA-based key exchange protocol. Link layer security can include both packet authentication between switches and MACsec encryption between switches (encryption is optional). Link layer security is supported on SAP-based MACsec.
Media Access Control Security and MACsec Key Agreement

MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP-TLS) or Pre Shared Key (PSK) framework.

A switch using MACsec accepts either MACsec or non-MACsec frames, depending on the policy associated with the MKA peer. MACsec frames are encrypted and protected with an integrity check value (ICV). When the switch receives frames from the MKA peer, it decrypts them and calculates the correct ICV by using session keys provided by MKA. The switch compares that ICV to the ICV within the frame. If they are not identical, the frame is dropped. The switch also encrypts and adds an ICV to any frames sent over the secured port (the access port used to provide the secure MAC service to a MKA peer) using the current session key.

The MKA Protocol manages the encryption keys used by the underlying MACsec protocol. The basic requirements of MKA are defined in 802.1x-REV. The MKA Protocol extends 802.1x to allow peer discovery with confirmation of mutual authentication and sharing of MACsec secret keys to protect data exchanged by the peers.

The EAP framework implements MKA as a newly defined EAP-over-LAN (EAPOL) packet. EAP authentication produces a master session key (MSK) shared by both partners in the data exchange. Entering the EAP session ID generates a secure connectivity association key name (CKN).

It generates a random secure association key (SAK), which is sent to the client partner. The client is never a key server and can only interact with a single MKA entity, the key server. After key derivation and generation, the switch sends periodic transports to the partner at a default interval of 2 seconds.

The packet body in an EAPOL Protocol Data Unit (PDU) is referred to as a MACsec Key Agreement PDU (MKPDU). MKA sessions and participants are deleted when the MKA lifetime (6 seconds) passes with no MKPDU received from a participant. For example, if a MKA peer disconnects, the participant on the switch continues to operate MKA until 6 seconds have elapsed after the last MKPDU is received from the MKA peer.

### Table 37: MACsec Support on Switch Ports

<table>
<thead>
<tr>
<th>Interface</th>
<th>Connections</th>
<th>MACsec support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Ports</td>
<td>Switch-to-host</td>
<td>MACsec MKA encryption</td>
</tr>
<tr>
<td>Uplink Ports</td>
<td>Switch-to-switch</td>
<td>MACsec MKA encryption, Cisco TrustSec NDAC MACsec</td>
</tr>
</tbody>
</table>

Cisco TrustSec and Cisco SAP are meant only for switch-to-switch links and are not supported on switch ports connected to end hosts, such as PCs or IP phones. MKA is supported on switch-to-host facing links and switch-to-switch facing links originating from the line card ports. Host-facing links typically use flexible authentication ordering for handling heterogeneous devices with or without IEEE 802.1x, and can optionally use MKA-based MACsec encryption. Cisco NDAC and SAP are mutually exclusive with Network Edge Access Topology (NEAT), which is used for compact switches to extend security outside the wiring closet.

Note: Integrity check value (ICV) indicator in MKPDU is optional. ICV is not optional when the traffic is encrypted.
MKA Policies

You apply a defined MKA policy to an interface to enable MKA on the interface. Removing the MKA policy disables MKA on that interface. You can configure these options:

- Policy name, not to exceed 16 ASCII characters.
- Confidentiality (encryption) offset of 0, 30, or 50 bytes for each physical interface

Virtual Ports

Use virtual ports for multiple secured connectivity associations on a single physical port. Each connectivity association (pair) represents a virtual port. In uplink, you can have only one virtual port per physical port. In downlink, you can have a maximum of two virtual ports per physical port, of which one virtual port can be part of a data VLAN; the other must externally tag its packets for the voice VLAN. You cannot simultaneously host secured and unsecured sessions in the same VLAN on the same port. Because of this limitation, 802.1x multiple authentication mode is not supported.

The exception to this limitation is in multiple-host mode when the first MACsec supplicant is successfully authenticated and connected to a hub that is connected to the switch. A non-MACsec host connected to the hub can send traffic without authentication because it is in multiple-host mode. We do not recommend using multi-host mode because after the first successful client, authentication is not required for other clients.

Virtual ports represent an arbitrary identifier for a connectivity association and have no meaning outside the MKA Protocol. A virtual port corresponds to a separate logical port ID. Valid port IDs for a virtual port are 0x0002 to 0xFFFF. Each virtual port receives a unique secure channel identifier (SCI) based on the MAC address of the physical interface concatenated with a 16-bit port ID.

MKA Statistics

Some MKA counters are aggregated globally, while others are updated both globally and per session. You can also obtain information about the status of MKA sessions.

MACsec, MKA and 802.1x Host Modes

You can use MACsec and the MKA Protocol with 802.1x single-host mode, multi-host mode, or Multi Domain Authentication (MDA) mode. Multiple authentication mode is not supported.

Single-Host Mode

The figure shows how a single EAP authenticated session is secured by MACsec by using MKA

Multiple Host Mode

In standard (not 802.1x REV) 802.1x multiple-host mode, a port is open or closed based on a single authentication. If one user, the primary secured client services client host, is authenticated, the same level of
network access is provided to any host connected to the same port. If a secondary host is a MACsec supplicant, it cannot be authenticated and traffic would not flow. A secondary host that is a non-MACsec host can send traffic to the network without authentication because it is in multiple-host mode. The figure shows MACsec in Standard Multiple-Host Unsecure Mode.

Figure 13: MACsec in Multiple-Host Mode - Unsecured

Note Multi-host mode is not recommended because after the first successful client, authentication is not required for other clients, which is not secure.

In standard (not 802.1x REV) 802.1x multiple-domain mode, a port is open or closed based on a single authentication. If the primary user, a PC on data domain, is authenticated, the same level of network access is provided to any domain connected to the same port. If a secondary user is a MACsec supplicant, it cannot be authenticated and traffic would no flow. A secondary user, an IP phone on voice domain, that is a non-MACsec host, can send traffic to the network without authentication because it is in multiple-domain mode.

Multiple-Domain Mode

In standard (not 802.1x REV) 802.1x multiple-domain mode, a port is open or closed based on a single authentication. If the primary user, a PC on data domain, is authenticated, the same level of network access is provided to any domain connected to the same port. If a secondary user is a MACsec supplicant, it cannot be authenticated and traffic would no flow. A secondary user, an IP phone on voice domain, that is a non-MACsec host, can send traffic to the network without authentication because it is in multiple-domain mode.

Information About MACsec MKA using EAP-TLS

Using IEE 802.1X Port-based Authentication with Extensible Authentication Protocol (EAP-TLS), you can configure MACsec MKA on the switch-to-switch links from the line card ports. EAP-TLS allows mutual authentication and obtains an MSK (master session key) from which the connectivity association key (CAK) is derived for MKA operations. Device certificates are carried, using EAP-TLS, for authentication to the AAA server.

Prerequisites for MACsec MKA using EAP-TLS

- Ensure that you have a Certificate Authority (CA) server configured for your network.
- Generate a CA certificate.
• Ensure that you have configured Cisco Identity Services Engine (ISE) Release 2.0.

• Ensure that both the participating devices, the CA server, and Cisco Identity Services Engine (ISE) are synchronized using Network Time Protocol (NTP). If time is not synchronized on all your devices, certificates will not be validated.

• Ensure that 802.1x authentication and AAA are configured on your device.

Information About MACsec Connection across Intermediate Switches

Prior to Cisco IOS XE Gibraltar 16.10.1, MACsec connection between end devices in a WAN MACsec deployment with the intermediate switches as the Cisco Catalyst 9000 Series Switches was not supported. The encrypted packets were dropped if WAN MACsec was configured on the end devices with MACsec not configured on the intermediate switches. With the ClearTag feature implemented on the ASIC, the switch forwards the encrypted packet without parsing the MACsec header. Below topology displays how the encrypted packets are forwarded through the intermediate switches with L2 switching.

Figure 14: Topology for ClearTag MACsec : MACsec not configured on the intermediate switches

Limitations for MACsec Connections across Intermediate Switches

• Hop-by-hop MACsec encryption with Catalyst 9000 Series switches as intermediate switches where WAN MACsec is configured on the routers is not supported.

• WAN MACsec configured on the routers with intermediate switches as the Catalyst 9000 Series switches is not supported on Layer 3 VPNs.

• WAN MACsec configured on the routers with intermediate switches as the Catalyst 9000 Series switches show CDP neighbors only in should-secure mode.

Information About MACsec Must Secure

Starting with Cisco IOS XE Fuji 16.8.1a, must-secure support is enabled on both the ingress and the egress. Must-secure is supported for MKA and SAP. With must-secure enabled, only EAPoL traffic will not be encrypted. The rest of the traffic will be encrypted. Unencrypted packets are dropped.
Must-secure mode is enabled by default.

Prior to Cisco IOS XE Fuji 16.8.1a, should-secure was supported for MKA and SAP. With should-secure enabled, if the peer is configured for MACsec, the data traffic is encrypted, otherwise it is sent in clear text.

**Information About MKA/MACsec for Port Channel**

MKA/MACsec can be configured on the port members of a port channel. MKA/MACsec is agnostic to the port channel since the MKA session is established between the port members of a port channel.

**Note**
Etherchannel links that are formed as part of the port channel can either be congruent or disparate i.e. the links can either be MACsec-secured or non-MACsec-secured. MKA session between the port members is established even if a port member on one side of the port channel is not configured with MACsec.

It is recommended that you enable MKA/MACsec on all the member ports for better security of the port channel.

**Information About MACsec Cipher Announcement**

Cipher Announcement allows the supplicant (AnyConnect) and the authenticator (the switch) to announce their respective MACsec Cipher Suite capabilities to each other. Supported Cipher Suites are GCM-AES-128 and GCM-AES-256. Both, the supplicant and the authenticator, calculate the largest common supported MACsec Cipher Suite and use the same as the keying material for the MKA session. Cisco AnyConnect Secure Mobility Client, Release 4.6.02074 and above support Cipher Announcement.

**Note**
Only the MACsec Cipher Suite capabilities which are configured in the MKA policy are announced from the authenticator (the switch) to the supplicant (AnyConnect).

On the supplicant side, you can choose the cipher suite(s) — GCM-AES-128 or GCM-AES-128 or both — in the Profile Editor section of the AnyConnect Network Access Manager. You can only choose the cipher suites if you select MKA from the drop-down list in the **Key Management** tab.

There are two types of EAPoL Announcements:

- **Unsecured Announcements (EAPoL PDUs):** Unsecured announcements are EAPoL announcements carrying MACsec Cipher Suite capabilities in an unsecured manner. These announcements are used to decide the width of the key used for MKA session prior to authentication.

- **Secure Announcements (MKPDUs):** Secure announcements revalidate the MACsec Cipher Suite capabilities which were shared previously through unsecure announcements.

Once the session is authenticated, peer capabilities which were received through EAPoL announcements are revalidated with the secure announcements. If there is a mismatch in the capabilities, the MKA session tears down.
Limitations for MACsec Cipher Announcement

- MACsec Cipher Announcement is supported only on the line card ports.
- If MACsec Cipher Suite Capabilities get changed in an active policy at the authenticator, the updated capabilities are not take into effect until a `shutdown/no shutdown` is performed on the interface. If you do not disable and restart the interface, EAPoL Announcement continues to announce the older capabilities.
- The MKA session between the supplicant and the authenticator does not tear down even if the MACsec Cipher Suite Capabilities configured on both do not result in a common cipher suite.

Cisco TrustSec Overview

The table below lists the TrustSec features to be eventually implemented on TrustSec-enabled Cisco switches. Successive general availability releases of TrustSec will expand the number of switches supported and the number of TrustSec features supported per switch.

<table>
<thead>
<tr>
<th>Cisco TrustSec Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1AE Tagging (MACsec)</td>
<td>Protocol for IEEE 802.1AE-based wire-rate hop-to-hop Layer 2 encryption.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This feature is only available between TrustSec hardware-capable devices.</td>
</tr>
<tr>
<td>Endpoint Admission Control (EAC)</td>
<td>EAC is an authentication process for an endpoint user or a device connecting to the TrustSec domain. Usually EAC takes place at the access level switch. Successful authentication and authorization in the EAC process results in Security Group Tag assignment for the user or device. Currently EAC can be 802.1X, MAC Authentication Bypass (MAB), and Web Authentication Proxy (WebAuth).</td>
</tr>
<tr>
<td>Network Device Admission Control (NDAC)</td>
<td>NDAC is an authentication process where each network device in the TrustSec domain can verify the credentials and trustworthiness of its peer device. NDAC utilizes an authentication framework based on IEEE 802.1X port-based authentication and uses EAP-FAST as its EAP method. Successful authentication and authorization in NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption.</td>
</tr>
</tbody>
</table>
Cisco TrustSec Feature | Description
--- | ---
Security Association Protocol (SAP) | 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.

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) | Security Group Tag Exchange Protocol (SXP). With SXP, devices that are not TrustSec-hardware-capable can receive SGT attributes for authenticated users and devices from the Cisco Identity Services Engine (ISE) or the Cisco Secure Access Control System (ACS). The devices can then forward a sourceIP-to-SGT binding to a TrustSec-hardware-capable device will tag the source traffic for SGACL enforcement.

When both ends of a link support 802.1AE MACsec, SAP negotiation occurs. An EAPOL-key exchange occurs between the supplicant and the authenticator to negotiate a cipher suite, exchange security parameters, and manage keys. Successful completion of these tasks results in the establishment of a security association (SA).

Depending on your software version and licensing and link hardware support, SAP negotiation can use one of these modes of operation:

- **Galois Counter Mode (GCM)**—authentication and encryption
- **GCM authentication (GMAC)**—GCM authentication, no encryption
- **No Encapsulation**—no encapsulation (clear text)
- **Null**—encapsulation, no authentication or encryption

### How to Configure MACsec Encryption

#### Configuring MKA and MACsec

By default, MACsec is disabled. No MKA policies are configured.

#### Configuring an MKA Policy

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Step 2</td>
<td>mka policy policy-name</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>key-server priority</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>include-icv-indicator</td>
</tr>
<tr>
<td>Step 5</td>
<td>macsec-cipher-suite</td>
</tr>
<tr>
<td></td>
<td>{gcm-aes-128</td>
</tr>
<tr>
<td>Step 6</td>
<td>confidentiality-offset</td>
</tr>
<tr>
<td></td>
<td>offset-value</td>
</tr>
<tr>
<td>Step 7</td>
<td>end</td>
</tr>
<tr>
<td>Step 8</td>
<td>show mka policy</td>
</tr>
</tbody>
</table>

**Configuring MACsec on an Interface**

Follow these steps to configure MACsec on an interface with one MACsec session for voice and one for data:
# Configuring MACsec on an Interface

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter the password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch&gt;enable</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch&gt;configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>interface interface-id</code></td>
<td>Identify the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.</td>
</tr>
<tr>
<td>4</td>
<td><code>switchport access vlan vlan-id</code></td>
<td>Configure the access VLAN for the port.</td>
</tr>
<tr>
<td>5</td>
<td><code>switchport mode access</code></td>
<td>Configure the interface as an access port.</td>
</tr>
<tr>
<td>6</td>
<td><code>macsec</code></td>
<td>Enable 802.1ae MACsec on the interface. The macsec command enables MKA MACsec on switch-to-host links (downlink ports) only.</td>
</tr>
<tr>
<td>7</td>
<td><code>access-session host-mode multi-host</code></td>
<td>Allows hosts to gain access to the interface.</td>
</tr>
<tr>
<td>8</td>
<td><code>access-session closed</code></td>
<td>Prevents preauthentication access on the interface.</td>
</tr>
<tr>
<td>9</td>
<td><code>access-session port-control auto</code></td>
<td>Sets the authorization state of a port.</td>
</tr>
<tr>
<td>10</td>
<td><code>authentication periodic</code></td>
<td>(Optional) Enable or Disable Reauthentication for this port.</td>
</tr>
<tr>
<td>11</td>
<td><code>authentication timer reauthenticate</code></td>
<td>(Optional) Enter a value between 1 and 65535 (in seconds). Obtains re-authentication timeout value from the server. Default re-authentication time is 3600 seconds.</td>
</tr>
<tr>
<td>12</td>
<td><code>authentication violation protect</code></td>
<td>Configure the port to drop unexpected incoming MAC addresses when a new device connects to a port or when a device connects to a port after the maximum number of devices are connected to that port. If not configured, the default is to shut down the port.</td>
</tr>
<tr>
<td>13</td>
<td><code>mka policy policy name</code></td>
<td>Apply an existing MKA protocol policy to the interface, and enable MKA on the interface. If no MKA policy was configured (by entering the <code>mka policy</code> global configuration command).</td>
</tr>
</tbody>
</table>
### Configuring MKA MACsec using PSK

#### Configuring MACsec MKA using PSK

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>key chain <em>key-chain-name</em> macsec</td>
</tr>
<tr>
<td>Step 3</td>
<td>key <em>hex-string</em></td>
</tr>
</tbody>
</table>
### Configuring MACsec MKA on an Interface using PSK

**Purpose**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>cryptographic-algorithm {gcm-aes-128</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>key-string { [0</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>lifetime local { start timestamp {hh::mm::ss</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
</tr>
</tbody>
</table>

### Configuring MACsec MKA on an Interface using PSK

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>macec network-link</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>mka policy policy-name</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>mka pre-shared-key key-chain key-chain name</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>macec replay-protection window-size frame number</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
</tr>
</tbody>
</table>

### Configuring MACsec MKA using EAP-TLS

To configure MACsec with MKA on point-to-point links, perform these tasks:

- Configure Certificate Enrollment
  - Generate Key Pairs
• Configure SCEP Enrollment
• Configure Certificates Manually
• Configure an Authentication Policy
• Configure EAP-TLS Profiles and IEEE 802.1x Credentials
• Configure MKA MACsec using EAP-TLS on Interfaces

Generating Key Pairs

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>crypto key generate rsa label label-name general-keys modulus size</td>
<td>Generates a RSA key pair for signing and encryption. You can also assign a label to each key pair using the label keyword. The label is referenced by the trustpoint that uses the key pair. If you do not assign a label, the key pair is automatically labeled &lt;Default-RSA-Key&gt;. If you do not use additional keywords this command generates one general purpose RSA key pair. If the modulus is not specified, the default key modulus of 1024 is used. You can specify other modulus sizes with the modulus keyword.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show authentication session interface interface-id</td>
<td>Verifies the authorized session security status.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Configuring Enrollment using SCEP

Simple Certificate Enrollment Protocol (SCEP) is a Cisco-developed enrollment protocol that uses HTTP to communicate with the certificate authority (CA) or registration authority (RA). SCEP is the most commonly used method for sending and receiving requests and certificates.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>cryptopki</strong> trustpoint <em>servername</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>enrollment url</strong> <em>url name pem</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifies the URL of the CA on which your device should send certificate requests.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>An IPv6 address can be added in the URL enclosed in brackets. For example: http://[2001:DB8:1:1::1]:80.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The pem keyword adds privacy-enhanced mail (PEM) boundaries to the certificate request.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>rsakeypair</strong> <em>label</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifies which key pair to associate with the certificate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The rsakeypair name must match the trust-point name.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>serial-number none</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The none keyword specifies that a serial number will not be included in the certificate request.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>ip-address none</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The none keyword specifies that no IP address should be included in the certificate request.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>revocation-check</strong> <strong>crl</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifies CRL as the method to ensure that the certificate of a peer has not been revoked.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>auto-enroll</strong> <em>percent regenerate</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enables auto-enrollment, allowing the client to automatically request a rollover certificate from the CA.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If auto-enrollment is not enabled, the client must be manually re-enrolled in your PKI upon certificate expiration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, only the Domain Name System (DNS) name of the device is included in the certificate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use the percent argument to specify that a new certificate will be requested after the percentage of the lifetime of the current certificate is reached.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use the regenerate keyword to generate a new key for the certificate even if a named key already exists.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the key pair is exportable: “! RSA key pair associated with trustpoint is exportable.”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>It is recommended that a new key pair be generated for security reasons.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> crypto pki authenticate name</td>
<td>Retrieves the CA certificate and authenticates it.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> exit</td>
<td>Exits global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> show crypto pki certificate trustpoint name</td>
<td>Displays information about the certificate for the trust point.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Enrollment Manually

If your CA does not support SCEP or if a network connection between the router and CA is not possible. Perform the following task to set up manual certificate enrollment:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> crypto pki trustpoint server name</td>
<td>Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> enrollment url url name pem</td>
<td>Specifies the URL of the CA on which your device should send certificate requests. An IPv6 address can be added in the URL enclosed in brackets. For example: http://[2001:DB8:1:1::1]:80. The pem keyword adds privacy-enhanced mail (PEM) boundaries to the certificate request.</td>
</tr>
<tr>
<td><strong>Step 4</strong> rsakeypair label</td>
<td>Specifies which key pair to associate with the certificate.</td>
</tr>
<tr>
<td><strong>Step 5</strong> serial-number none</td>
<td>The <code>none</code> keyword specifies that a serial number will not be included in the certificate request.</td>
</tr>
<tr>
<td><strong>Step 6</strong> ip-address none</td>
<td>The <code>none</code> keyword specifies that no IP address should be included in the certificate request.</td>
</tr>
<tr>
<td><strong>Step 7</strong> revocation-check crl</td>
<td>Specifies CRL as the method to ensure that the certificate of a peer has not been revoked.</td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits Global Configuration mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 9</strong> crypto pki authenticate <em>name</em></td>
<td>Retrieves the CA certificate and authenticates it.</td>
</tr>
<tr>
<td><strong>Step 10</strong> crypto pki enroll <em>name</em></td>
<td>Generates certificate request and displays the request for copying and pasting into the certificate server. Enter enrollment information when you are prompted. For example, specify whether to include the device FQDN and IP address in the certificate request. You are also given the choice about displaying the certificate request to the console terminal. The base-64 encoded certificate with or without PEM headers as requested is displayed.</td>
</tr>
<tr>
<td><strong>Step 11</strong> crypto pki import <em>name</em> <em>certificate</em></td>
<td>Imports a certificate via TFTP at the console terminal, which retrieves the granted certificate. The device attempts to retrieve the granted certificate via TFTP using the same filename used to send the request, except the extension is changed from “.req” to “.crt”. For usage key certificates, the extensions “-sign.crt” and “-encr.crt” are used. The device parses the received files, verifies the certificates, and inserts the certificates into the internal certificate database on the switch. <strong>Note</strong> Some CAs ignore the usage key information in the certificate request and issue general purpose usage certificates. If your CA ignores the usage key information in the certificate request, only import the general purpose certificate. The router will not use one of the two key pairs generated.</td>
</tr>
<tr>
<td><strong>Step 12</strong> exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 13</strong> show crypto pki certificate <em>trustpoint</em> <em>name</em></td>
<td>Displays information about the certificate for the trust point.</td>
</tr>
<tr>
<td><strong>Step 14</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Applying the 802.1x MACsec MKA Configuration on Interfaces

To apply MACsec MKA using EAP-TLS to interfaces, perform the following task:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Identifies the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.</td>
</tr>
<tr>
<td><strong>Step 3</strong> macsec network-link</td>
<td>Enables MACsec on the interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong> authentication periodic</td>
<td>(Optional) Enables reauthentication for this port.</td>
</tr>
<tr>
<td><strong>Step 5</strong> authentication timer reauthenticate interval</td>
<td>(Optional) Sets the reauthentication interval.</td>
</tr>
<tr>
<td><strong>Step 6</strong> access-session host-mode multi-host</td>
<td>Allows hosts to gain access to the interface.</td>
</tr>
<tr>
<td><strong>Step 7</strong> access-session closed</td>
<td>Prevents preauthentication access on the interface.</td>
</tr>
<tr>
<td><strong>Step 8</strong> access-session port-control auto</td>
<td>Sets the authorization state of a port.</td>
</tr>
<tr>
<td><strong>Step 9</strong> dot1x pae both</td>
<td>Configures the port as an 802.1X port access entity (PAE) supplicant and authenticator.</td>
</tr>
<tr>
<td><strong>Step 10</strong> dot1x credentials profile</td>
<td>Assigns a 802.1x credentials profile to the interface.</td>
</tr>
<tr>
<td><strong>Step 11</strong> dot1x supplicant eap profile name</td>
<td>Assigns the EAP-TLS profile to the interface.</td>
</tr>
<tr>
<td><strong>Step 12</strong> service-policy type control subscriber control-policy name</td>
<td>Applies a subscriber control policy to the interface.</td>
</tr>
<tr>
<td><strong>Step 13</strong> exit</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 14</strong> show macsec interface</td>
<td>Displays MACsec details for the interface.</td>
</tr>
<tr>
<td><strong>Step 15</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

### Configuring MKA/MACsec for Port Channel using PSK

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 macsec network-link</td>
<td>Enables MACsec on the interface. Supports layer 2 and layer 3 port channels.</td>
</tr>
<tr>
<td>Step 4 mka policy policy-name</td>
<td>Configures an MKA policy.</td>
</tr>
<tr>
<td>Step 5 mka pre-shared-key key-chain key-chain-name</td>
<td>Configures an MKA pre-shared-key key-chain name.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The MKA pre-shared key can be configured on either physical interface or sub-interfaces and not on both.</td>
</tr>
<tr>
<td>Step 6 macsec replay-protection window-size frame number</td>
<td>Sets the MACsec window size for replay protection.</td>
</tr>
<tr>
<td>Step 7 channel-group channel-group-number mode {auto</td>
<td>desirable}</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You cannot configure ports in a channel group without configuring MACsec on the interface. You must configure the commands in Step 3, 4, 5 and 6 before this step.</td>
</tr>
</tbody>
</table>

The channel-number range is from 1 to 4096. The port channel associated with this channel group is automatically created if the port channel does not already exist. For mode, select one of the following keywords:

- **auto** — Enables PAgP only if a PAgP device is detected. This places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation.

  **Note** The **auto** keyword is not supported when EtherChannel members are from different switches in the switch stack.

- **desirable** — Unconditionally enables PAgP. This places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets.
### Configuring Port Channel Logical Interfaces for Layer 2 EtherChannels

To create a port channel interface for a Layer 2 EtherChannel, perform this task:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 [no] interface port-channel
  channel-group-number | Creates the port channel interface. |
| Step 3 switchport | Switches an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration. |
| Step 4 switchport mode {access | trunk} | Assigns all ports as static-access ports in the same VLAN, or configure them as trunks. |
| Step 5 end | Returns to privileged EXEC mode. |

### Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels

To create a port channel interface for a Layer 3 EtherChannel, perform this task:
**Configuring MACsec Cipher Announcement**

**Configuring an MKA Policy for Secure Announcement**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> no switchport</td>
<td>Switches an interface that is in Layer 2 mode into Layer 3 mode for Layer 3 configuration.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip address ip-address subnet_mask</td>
<td>Assigns an IP address and subnet mask to the EtherChannel.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Note**

The default MACsec cipher suite in the MKA policy will always be "GCM-AES-128". If the device supports both "GCM-AES-128" and "GCM-AES-256" ciphers, it is highly recommended to define and use a user defined MKA policy to include both 128 and 256 bits ciphers or only 256 bits cipher, as may be required.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> mka policy policy-name</td>
<td>Identify an MKA policy, and enter MKA policy configuration mode. The maximum policy name length is 16 characters.</td>
</tr>
<tr>
<td><strong>Step 3</strong> key-server priority</td>
<td>Configure MKA key server options and set priority (between 0-255).</td>
</tr>
<tr>
<td><strong>Step 4</strong> [no] send-secure-announcements</td>
<td>Enables sending of secure announcements. Use the no form of the command to disable sending</td>
</tr>
</tbody>
</table>
### Configuring Secure Announcement Globally (Across all the MKA Policies)

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> [no] mka defaults policy send-secure-announcements</td>
<td>Enables sending of secure announcements in MKPDUs across MKA policies. By default, secure announcements are disabled.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Configuring EAPoL Announcements on an interface**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Identifies the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.</td>
</tr>
<tr>
<td><strong>Step 3</strong> [no] eapol announcement</td>
<td>Enable EAPoL announcements. Use the no form of the command to disable EAPoL announcements. By default, EAPoL announcements are disabled.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Configuring Cisco TrustSec MACsec

#### Configuring Cisco TrustSec Switch-to-Switch Link Security in Manual Mode

**Before you begin**

When manually configuring Cisco TrustSec on an interface, consider these usage guidelines and restrictions:
• If no SAP parameters are defined, Cisco TrustSec encapsulation or encryption is not performed.

• If you select GCM as the SAP operating mode, you must have a MACsec Encryption software license from Cisco. If you select GCM without the required license, the interface is forced to a link-down state.

• These protection levels are supported when you configure SAP pairwise master key (sap pmk):
  • SAP is not configured—no protection.
  • sap mode-list gcm-encrypt gmac no-encap—protection desirable but not mandatory.
  • sap mode-list gcm-encrypt gmac—confidentiality preferred and integrity required. The protection is selected by the supplicant according to supplicant preference.
  • sap mode-list gmac—integrity only.
  • sap mode-list gcm-encrypt—confidentiality required.
  • sap mode-list gmac gcm-encrypt—integrity required and preferred, confidentiality optional.

• Before changing the configuration from MKA to Cisco TrustSec SAP and vice versa, we recommend that you remove the interface configuration.

Beginning in privileged EXEC mode, follow these steps to manually configure Cisco TrustSec on an interface to another Cisco TrustSec device:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface tengigabitethernet 1/1/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>cts manual</td>
<td>Enters Cisco TrustSec manual configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# cts manual</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>sap pmk key [mode-list mode1 [mode2 [mode3 [mode4]]]]</td>
<td>(Optional) Configures the SAP pairwise master key (PMK) and operation mode. SAP is disabled by default in Cisco TrustSec manual mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>• <strong>gcm-encrypt</strong>—Authentication and encryption</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Select this mode for MACsec authentication and encryption if your software license supports MACsec encryption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>gmac</strong>—Authentication, no encryption</td>
</tr>
<tr>
<td></td>
<td>• <strong>no-encap</strong>—No encapsulation</td>
</tr>
<tr>
<td></td>
<td>• <strong>null</strong>—Encapsulation, no authentication or encryption</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the interface is not capable of data link encryption, <strong>no-encap</strong> is the default and the only available SAP operating mode. SGT is not supported.</td>
</tr>
</tbody>
</table>

**Step 5**  
**Example:**  
Switch(config-if-cts-manual)# **no propagate sgt**  
Use the **no** form of this command when the peer is incapable of processing a SGT. The **no propagate sgt** command prevents the interface from transmitting the SGT to the peer.

**Step 6**  
**Example:**  
Switch(config-if-cts-manual)# **exit**  
Exits Cisco TrustSec 802.1x interface configuration mode.

**Step 7**  
**Example:**  
Switch(config-if)# **end**  
Returns to privileged EXEC mode.

**Step 8**  
**Example:**  
Switch(config-if)# **show cts interface** [interface-id | brief | summary]  
(Optional) Verify the configuration by displaying TrustSec-related interface characteristics.

**Step 9**  
**Example:**  
Device#**copy running-config startup-config**  
(Optional) Saves your entries in the configuration file.
Configuring Examples for MACsec Encryption

Examples: Configuring MKA and MACsec

This example shows how to create an MKA policy:

```
Device# configure terminal
Device(config)# mka policy mka_policy
Device(config-mka-policy)# key-server priority 200
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Device(config-mka-policy)# confidentiality-offset 30
Device(config-mka-policy)# key-chain keychain1
Device(config-mka-policy)# enable
Device(config-mka-policy)# key-chain keychain1
Device(config-mka-policy)# key 1000
Device(config-mka-policy)# key-string 12345678901234567890123456789012
Device(config-mka-policy)# lifetime local 12:12:00 July 28 2016 12:19:00 July 28 2016
Device(config-mka-policy)# end
```

This example shows how to configure MACsec on an interface:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# switchport access vlan 1
Device(config-if)# switchport mode access
Device(config-if)# macsec
Device(config-if)# access-session event linksec fail action authorize vlan 1
Device(config-if)# access-session host-mode multi-domain
Device(config-if)# access-session linksec policy must-secure
Device(config-if)# authentication periodic
Device(config-if)# authentication timer reauthenticate
Device(config-if)# authentication violation protect
Device(config-if)# mka policy mka_policy
Device(config-if)# dot1x pae authenticator
Device(config-if)# spanning-tree portfast
Device(config-if)# end
```

Examples: Configuring MACsec MKA using PSK

This example shows how to configure MACsec MKA using PSK:

```
Device# configure terminal
Device(config)# Key chain keychain1 macsec
Device(config-keychain)# key 1000
Device(config-keychain)# cryptographic-algorithm gcm-aes-128
Device(config-keychain)# key-string 12345678901234567890123456789012
Device(config-keychain)# lifetime local 12:12:00 July 28 2016 12:19:00 July 28 2016
Device(config-keychain)# end
```

This example shows how to configure MACsec MKA on an interface using PSK:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# mka policy mka_policy
Device(config-if)# mka pre-shared-key key-chain key-chain-name
Device(config-if)# macsec replay-protection window-size 10
Device(config-if)# end
```

Examples: Configuring MACsec MKA using EAP-TLS

This example shows how to configure MACsec MKA using EAP-TLS:
Example: Configuring MACsec MKA for Port Channel using PSK

Etherchannel Mode — Static/On

The following is a sample configuration on Device 1 and Device 2 with EtherChannel Mode on.

```plaintext
key chain KC macsec
key 1000
  cryptographic-algorithm aes-128-cmac
  key-string FC8F5B10557C192F03F60198413D7D45
end

mka policy POLICY
  key-server priority 0
  macsec-cipher-suite gcm-aes-128
  confidentiality-offset 0
end
interface Te1/0/1
  channel-group 2 mode on
  macsec network-link
  mka policy POLICY
  mka pre-shared-key key-chain KC
end
interface Te1/0/2
  channel-group 2 mode on
  macsec network-link
  mka policy POLICY
  mka pre-shared-key key-chain KC
end
```

Layer 2 EtherChannel Configuration

Device 1

```plaintext
interface port-channel 2
  switchport
  switchport mode trunk
  no shutdown
end
```

Device 2

```plaintext
interface port-channel 2
  switchport
  switchport mode trunk
```
The following shows a sample output of `show etherchannel summary` command.

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

Number of channel-groups in use: 1  
Number of aggregators: 1  

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Po2(RU)</td>
<td>-</td>
<td>Te1/0/1(P) Te1/0/2(P)</td>
</tr>
</tbody>
</table>

Layer 3 EtherChannel Configuration

Device 1

```
interface port-channel 2
  no switchport
  ip address 10.25.25.3 255.255.255.0
  no shutdown
end
```

Device 2

```
interface port-channel 2
  no switchport
  ip address 10.25.25.4 255.255.255.0
  no shutdown
end
```

The following shows a sample output of `show etherchannel summary` command.

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

Number of channel-groups in use: 1
Number of aggregators: 1

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Po2(RU)</td>
<td>-</td>
<td>Tel/0/1(P)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel/0/2(P)</td>
</tr>
</tbody>
</table>

**Etherchannel Mode — LACP**

The following is a sample configuration on Device 1 and Device 2 with EtherChannel Mode as LACP.

```plaintext
key chain KC macsec
  key 1000
    cryptographic-algorithm aes-128-cmac
    key-string FC8F5B10557C192F03F60198413D7D45
  end
mka policy POLICY
  key-server priority 0
  macsec-cipher-suite gcm-aes-128
  confidentiality-offset 0
  end
interface Tel/0/1
  channel-group 2 mode active
  macsec network-link
  mka policy POLICY
  mka pre-shared-key key-chain KC
  end
interface Tel/0/2
  channel-group 2 mode active
  macsec network-link
  mka policy POLICY
  mka pre-shared-key key-chain KC
  end
```

**Layer 2 EtherChannel Configuration**

Device 1

```plaintext
interface port-channel 2
  switchport
  switchport mode trunk
  no shutdown
  end
```

Device 2
interface port-channel 2
switchport
switchport mode trunk
no shutdown
end

The following shows a sample output of `show etherchannel summary` command.

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

Number of channel-groups in use: 1
Number of aggregators: 1

---

2  Po2(SU)  LACP  Te1/1/1(P)  Te1/1/2(P)

Layer 3 EtherChannel Configuration

Device 1

interface port-channel 2
no switchport
ip address 10.25.25.3 255.255.255.0
no shutdown
end

Device 2

interface port-channel 2
no switchport
ip address 10.25.25.4 255.255.255.0
no shut

The following shows a sample output of `show etherchannel summary` command.

Flags:  D - down       P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3    S - Layer2
        U - in use    f - failed to allocate aggregator
        M - not in use, minimum links not met

Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)
Number of channel-groups in use: 1
Number of aggregators: 1

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Po2(RU)</td>
<td>LACP</td>
<td>Tel/1/1(P)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tel/1/2(P)</td>
</tr>
</tbody>
</table>

**Etherchannel Mode — PAgP**

The following is a sample configuration on Device 1 and Device 2 with EtherChannel Mode as PAgP.

```plaintext
key chain KC macsec
key 1000
  cryptographic-algorithm aes-128-cmac
  key-string FC8F5B10557C192F03F60198413D7D45
end

mka policy POLICY
key-server priority 0
macsec-cipher-suite gcm-aes-128
confidentiality-offset 0
end

interface Tel/0/1
  channel-group 2 mode desirable
  macsec network-link
  mka policy POLICY
  mka pre-shared-key key-chain KC
end

interface Tel/0/2
  channel-group 2 mode desirable
  macsec network-link
  mka policy POLICY
  mka pre-shared-key key-chain KC
end
```

**Layer 2 EtherChannel Configuration**

Device 1

```plaintext
interface port-channel 2
  switchport
  switchport mode trunk
  no shutdown
end
```

Device 2
interface port-channel 2
switchport
switchport mode trunk
no shutdown
end

The following shows a sample output of `show etherchannel summary` command.

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

A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1

-----------------------------------------------
  2  Po2(SU)  PAgP  Tel/1/1(P)  Tel/1/2(P)
-----------------------------------------------

Layer 3 EtherChannel Configuration

Device 1

interface port-channel 2
no switchport
ip address 10.25.25.3 255.255.255.0
no shutdown
end

Device 2

interface port-channel 2
no switchport
ip address 10.25.25.4 255.255.255.0
no shutdown
end

The following shows a sample output of `show etherchannel summary` command.

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

---

Example: Configuring MACsec MKA for Port Channel using PSK

MACsec Encryption
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Displaying Active MKA Sessions
The following shows all the active MKA sessions.

Device# show mka sessions interface Te1/0/1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Local-TxSCI</th>
<th>Policy-Name</th>
<th>Inherited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key-Server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port-ID</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key-Server</th>
<th>Port-ID</th>
<th>Peer-RxSCI</th>
<th>MACsec-Peers</th>
<th>Status</th>
<th>CKN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Te1/0/1</td>
<td>00a3.d144.3364/0025</td>
<td>POLICY</td>
<td>NO</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>701f.539b.b0c6/0032</td>
<td>1</td>
<td>Secured</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Examples: Configuring MACsec Cipher Announcement

This example shows how to configure MKA policy for Secure Announcement:

Device# configure terminal
Device(config)# mka policy mka_policy
Device(config-mka-policy)# key-server 2
Device(config-mka-policy)# send-secure-announcements
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128confidentiality-offset 0
Device(config-mka-policy)# end

This example shows how to configure Secure Announcement globally:

Device# configure terminal
Device(config)# mka defaults policy send-secure-announcements
Device(config)# end

This example shows how to configure EAPoL Announcements on an interface:

Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# eapol announcement
Device(config-if)# end
The following is a sample output for `show running-config interface interface-name` command with EAPoL announcement enabled.

```
Device# show running-config interface GigabitEthernet 1/0/1
switchport mode access
  macsec
    access-session host-mode multi-host
    access-session closed
    access-session port-control auto
  dot1x pae authenticator
    dot1x timeout quiet-period 10
    dot1x timeout tx-period 5
    dot1x timeout supp-timeout 10
    dot1x supplicant eap profile peap
eapol announcement
  spanning-tree portfast
  service-policy type control subscriber Dot1X
```

The following is a sample output of the `show mka sessions interface interface-name detail` command with secure announcement disabled.

```
Device# show mka sessions interface GigabitEthernet 1/0/1 detail

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI............. 204c.9e85.ede4/002b
Interface MAC Address.... 204c.9e85.ede4
MKA Port Identifier...... 43
Interface Name........... GigabitEthernet1/0/1
Audit Session ID...........
CAK Name (CKN)...........
0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5D675945CEAE
Message Number (MN)...... 89567
EAP Role.................. NA
Key Server................. YES
MKA Cipher Suite......... AES-128-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............. 0
Latest SAK KI (KN)........ D46CBEC05D5D675945CEAE00000001 (1)
Old SAK Status............ FIRST-SAK
Old SAK AN................ 0
Old SAK KI (KN)............ FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)

MKA Policy Name........... p2
Key Server Priority...... 2
```
Delay Protection........... NO
Replay Protection......... YES
Replay Window Size........ 0
Confidentiality Offset... 0
Algorithm Agility......... 80C201
Send Secure Announcement.. DISABLED
SAK Cipher Suite......... 0080C20010000001 (GCM-AES-128)
MACsec Capability......... 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired............ YES

# of MACsec Capable Live Peers........... 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
<table>
<thead>
<tr>
<th>MI</th>
<th>MN</th>
<th>Rx-SCI (Peer)</th>
<th>KS Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0100000000000000000000000000000000000000000000000000000000000000</td>
<td>38046BA37D7DA77E06D006A9</td>
<td>89555</td>
<td>c800.8459.e764/002a</td>
</tr>
</tbody>
</table>

Potential Peers List:
<table>
<thead>
<tr>
<th>MI</th>
<th>MN</th>
<th>Rx-SCI (Peer)</th>
<th>KS Priority</th>
</tr>
</thead>
</table>

Dormant Peers List:

The following is a sample output of the `show mka sessions details` command with secure announcement disabled.

```
Device# show mka sessions details
MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec
Local Tx-SCI............. 204c.9e85.e6e4/002b
Interface MAC Address.... 204c.9e85.e6e4
MKA Port Identifier...... 43
Interface Name.......... GigabitEthernet1/0/1
Audit Session ID........
CAK Name (CKN).......... 0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC056D557543CEAE
Message Number (MN)..... 89572
EAP Role................. NA
Key Server............... YES
MKA Cipher Suite......... AES-128-CMAC

Latest SAK Status....... Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... D46CBEC056D557543CEAE00000001 (1)
Old SAK Status.......... FIRST-SAK
Old SAK AN............. 0
Old SAK KI (KN)......... FIRST-SAK (0)
```

Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)
SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time........... 0s (No Old SAK to retire)

MKA Policy Name.......... p2
Key Server Priority....... 2
Delay Protection.......... NO
Replay Protection......... YES
Replay Window Size....... 0
Confidentiality Offset... 0
Algorithm Agility........ 80C201
Send Secure Announcement.. DISABLED
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired.......... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
MI      MN      Rx-SCI (Peer)      KS Priority
--------- ------- ----------------- ------------
38046BA37D7DA77E06D006A9  89560   c800.8459.e764/002a  10

Potential Peers List:
MI      MN      Rx-SCI (Peer)      KS Priority
--------- ------- ----------------- ------------

Dormant Peers List:
MI      MN      Rx-SCI (Peer)      KS Priority
--------- ------- ----------------- ------------

The following is a sample output of the `show mka policy policy-name detail` command with secure announcement disabled.

```
Device# show mka policy p2 detail
MKA Policy Configuration ("p2")
-----------------------------
MKA Policy Name.......... p2
Key Server Priority....... 2
Confidentiality Offset... 0
Send Secure Announcement..DISABLED
Cipher Suite(s)......... GCM-AES-128

Applied Interfaces...
    GigabitEthernet1/0/1
```

**Examples : Cisco TrustSec Switch-to-Switch Link Security**

This example shows the configuration necessary for a seed and non-seed device for Cisco TrustSec switch-to-switch security. You must configure the AAA and RADIUS for link security. In this example, ACS-1 through ACS-3 can be any server names and cts-radius is the Cisco TrustSec server.
Seed Device Configuration:

Switch(config)#aaa new-model
Switch(config)#radius server ACS-1
Switch(config-radius-server)#address ipv4 10.5.120.12 auth-port 1812 acct-port 1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#radius server ACS-2
Switch(config-radius-server)#address ipv4 10.5.120.14 auth-port 1812 acct-port 1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#radius server ACS-3
Switch(config-radius-server)#address ipv4 10.5.120.15 auth-port 1812 acct-port 1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#aaa group server radius cts-radius
Switch(config-sg-radius)#server name ACS-1
Switch(config-sg-radius)#server name ACS-2
Switch(config-sg-radius)#server name ACS-3
Switch(config-sg-radius)#exit
Switch(config)#aaa authentication login default none
Switch(config)#aaa authentication dot1x default group cts-radius
Switch(config)#aaa authorization network cts-radius group cts-radius
Switch(config)#aaa session-id common
Switch(config)#cts authorization list cts-radius
Switch(config)#dot1x system-auth-control
Switch(config)#interface gi1/1/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#cts dot1x
Switch(config-if-cts-dot1x)#sap mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)#exit
Switch(config-if)#exit
Switch(config)#interface gi1/1/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#cts manual
Switch(config-if-cts-dot1x)#sap pmk 03345AABBCCDDEEFF mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)#no propagate sgt
Switch(config-if-cts-dot1x)#exit
Switch(config-if)#exit
Switch(config)#radius-server vsa send authentication
Switch(config)#end
Switch#cts credentials id cts-36 password trustsec123

Non-Seed Device:
Examples: Displaying MKA Statistics

The following is a sample output of the `show mka sessions` command.

```
Device# show mka sessions

Total MKA Sessions....... 1
  Secured Sessions... 1
  Pending Sessions... 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Local-TxSCI</th>
<th>Policy-Name</th>
<th>Inherited</th>
<th>Key-Server</th>
<th>Peer-RxSCI</th>
<th>MACsec-Peers</th>
<th>Status</th>
<th>CKN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>204c.9e85.ede4/002b p2</td>
<td>p2</td>
<td>NO</td>
<td>43</td>
<td>c800.8459.e764/002a 1</td>
<td>Secured</td>
<td>YES</td>
<td></td>
</tr>
</tbody>
</table>

The following is a sample output of the `show mka sessions interface interface-name` command.
Device# show mka sessions interface GigabitEthernet 1/0/1

Summary of All Currently Active MKA Sessions on Interface GigabitEthernet1/0/1...

---

<table>
<thead>
<tr>
<th>Interface</th>
<th>Local-TxSCI</th>
<th>Policy-Name</th>
<th>Inherited</th>
<th>Key-Server Port-ID</th>
<th>Peer-RxSCI MACsec-Peers Status</th>
<th>CKN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>204c.9e85.ede4/002b p2</td>
<td>YES</td>
<td>NO</td>
<td>43</td>
<td>c800.8459.e764/002a</td>
<td>Secured</td>
</tr>
<tr>
<td></td>
<td>0100000000000000000000000000000000000000000000000000000000000000</td>
<td>1</td>
<td>0100000000000000000000000000000000000000000000000000000000000000</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following is a sample output of the show mka sessions interface interface-name detail command.

Device# show mka sessions interface GigabitEthernet 1/0/1 detail

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI............. 204c.9e85.ede4/002b
Interface MAC Address.... 204c.9e85.ede4
MKA Port Identifier...... 43
Interface Name........... GigabitEthernet1/0/1
Audit Session ID..........
CAK Name (CKN)........... 0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5D67594543CEAE
Message Number (MN)..... 89567
EAP Role............... NA
Key Server............... YES
MKA Cipher Suite......... AES-128-CMAC

Latest SAK Status....... Rx & Tx
Latest SAK AN............. 0
Latest SAK KI (KN)....... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status.......... FIRST-SAK
Old SAK AN............. 0
Old SAK KI (KN).......... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time......... 0s (No Old SAK to retire)

MKA Policy Name........... p2
Key Server Priority...... 2
Delay Protection......... NO
Replay Protection......... YES
Replay Window Size....... 0
Confidentiality Offset... 0
Algorithm Agility........ 80C201
Send Secure Announcement.. DISABLED
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired......... YES

# of MACsec Capable Live Peers......... 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
MI   MN                        Rx-SCI (Peer)   KS Priority
--------------------------------------------------------------------------------
38046BA37D7DA77E06D006A9  89555               c800.8459.e764/002a  10

Potential Peers List:
MI   MN                        Rx-SCI (Peer)   KS Priority
--------------------------------------------------------------------------------

Dormant Peers List:
MI   MN                        Rx-SCI (Peer)   KS Priority
--------------------------------------------------------------------------------

The following is a sample output of the `show mka sessions details` command.

```
Device# show mka sessions details
MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI............ 204c.9e85.ede4/002b
Interface MAC Address.... 204c.9e85.ede4
MKA Port Identifier...... 43
Interface Name........... GigabitEthernet1/0/1
Audit Session ID.........
CAK Name (CKN)........... 0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5D67594543CEAE
Message Number (MN)...... 89572
EAP Role.................. NA
Key Server................ YES
MKA Cipher Suite......... AES-128-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............... 0
Latest SAK KI (KN)....... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status........... FIRST-SAK
Old SAK AN............... 0
Old SAK KI (KN).......... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time......... 0s (No Old SAK to retire)

MKA Policy Name......... p2
Key Server Priority...... 2
```
Delay Protection........ NO
Replay Protection........ YES
Replay Window Size........ 0
Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Cipher Suite......... 0080C2000100001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
<table>
<thead>
<tr>
<th>MI</th>
<th>MN</th>
<th>Rx-SCI (Peer)</th>
<th>KS Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>38046BA37D7DA77E06D006A9</td>
<td>89560</td>
<td>c800.8459.e764/002a</td>
<td>10</td>
</tr>
</tbody>
</table>

Potential Peers List:

Dormant Peers List:

The following is a sample output of the `show mka policy` command.

```
Device# show mka policy

MKA Policy Summary...

Policy Interfaces Name Applied
KS Delay Replay Window Conf Cipher Priority Protect Protect Size Offset Suite(s)
<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>NAME</th>
<th>PRIOR</th>
<th>PROTECT</th>
<th>PROTECT</th>
<th>SIZE</th>
<th>OFFSET</th>
<th>SUITE(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>DEFAULT POLICY</em></td>
<td>0</td>
<td>FALSE</td>
<td>TRUE</td>
<td>0</td>
<td>0</td>
<td>GCM-AES-128</td>
</tr>
<tr>
<td></td>
<td>p1</td>
<td>1</td>
<td>FALSE</td>
<td>TRUE</td>
<td>0</td>
<td>0</td>
<td>GCM-AES-128</td>
</tr>
<tr>
<td></td>
<td>p2</td>
<td>2</td>
<td>FALSE</td>
<td>TRUE</td>
<td>0</td>
<td>0</td>
<td>GCM-AES-128</td>
</tr>
<tr>
<td></td>
<td>Gi1/0/1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

The following is a sample output of the `show mka policy policy-name` command.

```
Device# show mka policy p2

MKA Policy Summary...

Policy Interfaces Name Applied
KS Delay Replay Window Conf Cipher Priority Protect Protect Size Offset Suite(s)
<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>NAME</th>
<th>PRIOR</th>
<th>PROTECT</th>
<th>PROTECT</th>
<th>SIZE</th>
<th>OFFSET</th>
<th>SUITE(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>DEFAULT POLICY</em></td>
<td>0</td>
<td>FALSE</td>
<td>TRUE</td>
<td>0</td>
<td>0</td>
<td>GCM-AES-128</td>
</tr>
<tr>
<td></td>
<td>p1</td>
<td>1</td>
<td>FALSE</td>
<td>TRUE</td>
<td>0</td>
<td>0</td>
<td>GCM-AES-128</td>
</tr>
<tr>
<td></td>
<td>p2</td>
<td>2</td>
<td>FALSE</td>
<td>TRUE</td>
<td>0</td>
<td>0</td>
<td>GCM-AES-128</td>
</tr>
<tr>
<td></td>
<td>Gi1/0/1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The following is a sample output of the `show mka policy policy-name detail` command.

Device# show mka policy p2 detail
MKA Policy Configuration ("p2")
==================================
MKA Policy Name........ p2
Key Server Priority.... 2
Confidentiality Offset. 0
Send Secure Announcement..DISABLED
Cipher Suite(s)........ GCM-AES-128

Applied Interfaces...
  GigabitEthernet1/0/1

The following is a sample output of the `show mka statistics interface interface-name` command.

Device# show mka statistics interface GigabitEthernet 1/0/1

MKA Statistics for Session
==================================
Reauthentication Attempts.. 0

CA Statistics
  Pairwise CAKs Derived... 0
  Pairwise CAK Rekeys..... 0
  Group CAKs Generated.... 0
  Group CAKs Received..... 0

SA Statistics
  SAKs Generated......... 1
  SAKs Rekeyed............ 0
  SAKs Received........... 0
  SAK Responses Received.. 1

MKPDU Statistics
  MKPDUs Validated & Rx... 89585
    "Distributed SAK".. 0
    "Distributed CAK".. 0
  MKPDUs Transmitted...... 89596
    "Distributed SAK".. 1
    "Distributed CAK".. 0

The following is a sample output of the `show mka summary` command.

Device# show mka summary
Total MKA Sessions....... 1
  Secured Sessions... 1
  Pending Sessions... 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Local-TxSCI</th>
<th>Policy-Name</th>
<th>Inherited</th>
</tr>
</thead>
</table>

Examples: Displaying MKA Statistics
### Key-Server

<table>
<thead>
<tr>
<th>Port-ID</th>
<th>Peer-RxSCI</th>
<th>MACsec-Peers</th>
<th>Status</th>
<th>CKN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>204c.9e85.ede4/002b p2</td>
<td>NO</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>c800.8459.e764/002a 1</td>
<td>Secured</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0100000000000000000000000000000000000000000000000000000000000000</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### MKA Global Statistics

**- MKA Session Totals**
- Secured.................... 1
- Reauthentication Attempts.. 0
- Deleted (Secured)........... 0
- Keepalive Timeouts......... 0

**- CA Statistics**
- Pairwise CAKs Derived...... 0
- Pairwise CAK Rekeys........ 0
- Group CAKs Generated....... 0
- Group CAKs Received........ 0

**- SA Statistics**
- SAKs Generated............... 1
- SAKs Rekeyed.................. 0
- SAKs Received................. 0
- SAK Responses Received....... 1

**- MKPDU Statistics**
- MKPDUs Validated & Rx....... 89589
  - "Distributed SAK"....... 0
  - "Distributed CAK"...... 0
- MKPDUs Transmitted........... 89600
  - "Distributed SAK"...... 1
  - "Distributed CAK"..... 0

**- MKA Error Counter Totals**

**- Session Failures**
- Bring-up Failures............... 0
- Reauthentication Failures...... 0
- Duplicate Auth-Mgr Handle....... 0

**- SAK Failures**
- SAK Generation................... 0
- Hash Key Generation.............. 0
- SAK Encryption/Wrap............... 0
- SAK Decryption/Unwrap............ 0
- SAK Cipher Mismatch.............. 0
CA Failures
   Group CAK Generation............. 0
   Group CAK Encryption/Wrap......... 0
   Group CAK Decryption/Unwrap...... 0
   Pairwise CAK Derivation........... 0
   CKN Derivation.................... 0
   ICK Derivation.................... 0
   KEK Derivation.................... 0
   Invalid Peer MACsec Capability... 0

MACsec Failures
   Rx SC Creation..................... 0
   Tx SC Creation..................... 0
   Rx SA Installation................ 0
   Tx SA Installation................ 0

MKPDU Failures
   MKPDU Tx........................... 0
   MKPDU Rx Validation................. 0
   MKPDU Rx Bad Peer MN................ 0
   MKPDU Rx Non-recent Peerlist MN.... 0
Configuring Secure Shell

- Prerequisites for Configuring Secure Shell, on page 221
- Restrictions for Configuring Secure Shell, on page 222
- Information About Configuring Secure Shell, on page 222
- How to Configure Secure Shell, on page 224
- Monitoring the SSH Configuration and Status, on page 228
- Feature Information for Secure Shell, on page 228

Prerequisites for Configuring Secure Shell

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

- For SSH to work, the switch needs an Rivest, Shamir, and Adleman (RSA) public/private key pair. This is the same with Secure Copy Protocol (SCP), which relies on SSH for its secure transport.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.

- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.

- SCP relies on SSH for security.

- SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.

- 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.

- The Secure Shell (SSH) server requires an IPsec (Data Encryption Standard [DES] or 3DES) encryption software image; the SSH client requires an IPsec (DES or 3DES) encryption software image.

- Configure a hostname and host domain for your device by using the hostname and ip domain-name commands in global configuration mode.
Restrictions for Configuring Secure Shell

The following are restrictions for configuring the Device for secure shell.

- The switch supports Rivest, Shamir, and Adelman (RSA) authentication.

- SSH supports only the execution-shell application.

- The SSH server and the SSH client are supported only on Data Encryption Standard (DES) (56-bit) and 3DES (168-bit) data encryption software. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.

- The Device supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.

- When using SCP, you cannot enter the password into the `copy` command. You must enter the password when prompted.

- The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2.

- The `-l` keyword and `userid : {number} {ip-address}` delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for console access.

Information About Configuring Secure Shell

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 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 2 (SSHv2).

SSH functions the same in IPv6 as in IPv4. For IPv6, SSH supports IPv6 addresses and enables secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

SSH Servers, Integrated Clients, and Supported Versions

The Secure Shell (SSH) Integrated Client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco device to make a secure, encrypted connection to another Cisco device or to any other device running the SSH server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for secure communication over an unsecured network.

The SSH server and SSH integrated client are applications that run on the switch. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), 3DES, and password authentication.
The SSH client functionality is available only when the SSH server is enabled.

User authentication is performed like that in the Telnet session to the device. SSH also supports the following user authentication methods:

- TACACS+
- RADIUS
- Local authentication and authorization

### 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.

### 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.
Secure Copy Protocol

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying device 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 device can determine whether the user has the correct privilege level. To configure the Secure Copy feature, you should understand the SCP concepts.

How to Configure Secure Shell

Setting Up the Device to Run SSH

Follow the procedure given below to set up your Device to run SSH:

Before you begin

Configure user authentication for local or remote access. This step is required. For more information, see Related Topics below.

Procedure

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

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

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>hostname hostname</td>
<td>Configures a hostname and IP domain name for your Device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# hostname your_hostname</td>
<td></td>
</tr>
</tbody>
</table>

Note: Follow this procedure only if you are configuring the Device as an SSH server.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td><code>ip domain-name domain_name</code></td>
<td>Configures a host domain for your Device.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# <code>ip domain-name your_domain</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>crypto key generate rsa</code></td>
<td>Enables the SSH server for local and remote authentication on the Device and generates an RSA key pair. Generating an RSA key pair for the Device automatically enables SSH.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# <code>crypto key generate rsa</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>We recommend that a minimum modulus size of 1024 bits.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Follow this procedure only if you are configuring the Device as an SSH server.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# <code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# <code>copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the SSH Server

Follow these steps to configure the SSH server:
This procedure is only required if you are configuring the Device as an SSH server.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `enable` | Enables privileged EXEC mode.  
  * Enter your password if prompted. |
| **Example:** |  
  Device> `enable` |  |
| **Step 2** | `configure terminal` | Enters global configuration mode. |
| **Example:** |  
  Device# `configure terminal` |  |
| **Example:** |  
  Device(config)# `ip ssh version 2` |  |
| **Step 4** | `ip ssh {timeout seconds | authentication-retries number}` | Configures the SSH control parameters:  
  * Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the Device uses the default time-out values of the CLI-based sessions.  
  By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the CLI-based session time-out value returns to the default of 10 minutes.  
  * Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5.  
  Repeat this step when configuring both parameters. |
| **Example:** |  
  Device(config)# `ip ssh timeout 90`  
  Device(config)# `ip ssh authentication-retries 2` |  |
| Step 5 | Use one or both of the following:  
| • line vty  
| line_number[ending_line_number]  
| • transport input ssh  
**Example:**  
Device(config)# line vty 1 10  
or  
Device(config-line)# transport input ssh | (Optional) Configures the virtual terminal line settings.  
• Enters line configuration mode to configure the virtual terminal line settings.  
For the line_number and ending_line_number arguments, the range is from 0 to 15.  
• Specifies that the Device prevents non-SSH Telnet connections, limiting the device to only SSH connections. |
| Step 6 | end  
**Example:**  
Device(config-line)# end | Exits line configuration mode and returns to privileged EXEC mode. |
| Step 7 | Use one of the following:  
| • show ip ssh  
| • show ssh  
**Example:**  
Device# show ip ssh  
or  
Device# show ssh | • Shows the version and configuration information for your SSH server.  
• Shows the status of the SSH server connections on the Device. |
| Step 8 | show running-config  
**Example:**  
Device# show running-config | Verifies your entries. |
| Step 9 | copy running-config startup-config  
**Example:**  
Device# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |
Monitoring the SSH Configuration and Status

This table displays the SSH server configuration and status.

Table 38: Commands for Displaying the SSH Server Configuration and Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ssh</td>
<td>Shows the version and configuration information for the SSH server.</td>
</tr>
<tr>
<td>show ssh</td>
<td>Shows the status of the SSH server.</td>
</tr>
</tbody>
</table>

Feature Information for Secure Shell

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 39: Feature Information for Secure Shell

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Shell</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>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 SSHv2.</td>
</tr>
</tbody>
</table>
Configuring SSH File Transfer Protocol

Secure Shell (SSH) includes support for SSH File Transfer Protocol (SFTP), which is a new standard file transfer protocol introduced in SSHv2. This feature provides a secure and authenticated method for copying device configuration or device image files.

- Prerequisites for SSH File Transfer Protocol, on page 229
- Restrictions for SSH File Transfer Protocol, on page 229
- Information About SSH File Transfer Protocol, on page 229
- How to Configure SSH File Transfer Protocol, on page 230
- Example: Configuring SSH File Transfer Protocol, on page 231
- Additional References, on page 231
- Feature Information for SSH File Transfer Protocol, on page 232

Prerequisites for SSH File Transfer Protocol

- SSH must be enabled.
- The `ip ssh source-interface interface-type interface-number` command must be configured.

Restrictions for SSH File Transfer Protocol

- The SFTP server is not supported.
- SFTP boot is not supported.
- The `sftp` option in the `install add` command is not supported.

Information About SSH File Transfer Protocol

The SFTP client functionality is provided as part of the SSH component and is always enabled on the corresponding device. Therefore, any SFTP server user with the appropriate permission can copy files to and from the device.

An SFTP client is VRF-aware; you can configure the secure FTP client to use the virtual routing and forwarding (VRF) associated with a particular source interface during connection attempts.
How to Configure SSH File Transfer Protocol

The following sections provide information about the various tasks that comprise an SFTP configuration.

Configuring SFTP

Perform the following steps:

Before you begin

To configure a Cisco device for SFTP client-side functionality, the `ip ssh source-interface interface-type interface-number` command must be configured first.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip ssh source-interface interface-type interface-number</td>
<td>Defines the source IP for the SSH session.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ip ssh source-interface GigabitEthernet 1/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
<td>(Optional) Displays the SFTP client-side functionality.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>debug ip sftp</td>
<td>(Optional) Enables SFTP debugging.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# debug ip sftp</td>
<td></td>
</tr>
</tbody>
</table>
Perform an SFTP Copy Operation

SFTP copy takes the IP or hostname of the corresponding server if Domain Name System (DNS) is configured. To perform SFTP copy operations, use the following commands in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# <code>copy ios-file-system:file sftp://user:pwd@server-ip//filepath</code></td>
<td>Copies a file from the local Cisco IOS file system to the server.</td>
</tr>
<tr>
<td>Or</td>
<td>Specify the username, password, IP address, and filepath of the server.</td>
</tr>
<tr>
<td>Device# <code>copy ios-file-system: sftp:</code></td>
<td></td>
</tr>
<tr>
<td>Device# <code>copy sftp://user:pwd@server-ip//filepath ios-file-system:file</code></td>
<td>Copies the file from the server to the local Cisco IOS file system.</td>
</tr>
<tr>
<td>Or</td>
<td>Specify the username, password, IP address, and filepath of the server.</td>
</tr>
<tr>
<td>Device# <code>copy sftp: ios-file-system:</code></td>
<td></td>
</tr>
</tbody>
</table>

Example: Configuring SSH File Transfer Protocol

The following example shows how to configure the client-side functionality of SFTP:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh source-interface gigabitethernet 1/0/1
Device(config)# exit
```

Additional References

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Secure Shell Version 1 and 2 Support</td>
<td>Secure Shell Configuration Guide</td>
</tr>
</tbody>
</table>
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.

---

**Feature Information for SSH File Transfer Protocol**

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH File Transfer Protocol (SFTP)</td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>SSH includes support for SFTP, a new standard file transfer protocol introduced in SSHv2.</td>
</tr>
</tbody>
</table>
X.509v3 Certificates for SSH Authentication

The X.509v3 Certificates for SSH Authentication feature uses the X.509v3 digital certificates in server and user authentication at the secure shell (SSH) server side.

This module describes how to configure server and user certificate profiles for a digital certificate.

Prerequisites for X.509v3 Certificates for SSH Authentication

- The X.509v3 Certificates for SSH Authentication feature introduces the `ip ssh server algorithm authentication` command to replace the `ip ssh server authenticate user` command. If you use the `ip ssh server authenticate user` command, the following deprecation message is displayed.

  Warning: SSH command accepted but this CLI will be deprecated soon. Please move to new CLI “ip ssh server algorithm authentication”. Please configure “default ip ssh server authenticate user” to make CLI ineffective.

- Use the `default ip ssh server authenticate user` command to remove the `ip ssh server authenticate user` command from effect. The IOS secure shell (SSH) server then starts using the `ip ssh server algorithm authentication` command.

Restrictions for X.509v3 Certificates for SSH Authentication

- The X.509v3 Certificates for SSH Authentication feature implementation is applicable only on the IOS secure shell (SSH) server side.

- IOS SSH server supports only the `x509v3-ssh-rsa` algorithm based certificate for server and user authentication on the IOS SSH server side.
Information About X.509v3 Certificates for SSH Authentication

The following section provides information about digital certificates, and server and user authentication.

Digital Certificates

The validity of the authentication depends upon the strength of the linkage between the public signing key and the identity of the signer. Digital certificates in the X.509v3 format (RFC5280) are used to provide identity management. A chain of signatures by a trusted root certification authority and its intermediate certificate authorities binds a given public signing key to a given digital identity.

Public key infrastructure (PKI) trustpoint helps manage the digital certificates. The association between the certificate and the trustpoint helps track the certificate. The trustpoint contains information about the certificate authority (CA), different identity parameters, and the digital certificate. Multiple trustpoints can be created to associate with different certificates.

Server and User Authentication using X.509v3

For server authentication, the IOS secure shell (SSH) server sends its own certificate to the SSH client for verification. This server certificate is associated with the trustpoint configured in the server certificate profile (ssh-server-cert-profile-server configuration mode).

For user authentication, the SSH client sends the user's certificate to the IOS SSH server for verification. The SSH server validates the incoming user certificate using public key infrastructure (PKI) trustpoints configured in the server certificate profile (ssh-server-cert-profile-user configuration mode).

By default, certificate-based authentication is enabled for server and user at the IOS SSH server end.

How to Configure X.509v3 Certificates for SSH Authentication

The following section provides information about how to configure X.509v3 Certificates for SSH Authentication.

Configuring IOS SSH Server to Use Digital Certificates for Server Authentication

To configure IOS SSH server to use digital certificates for server authentication, perform this procedure:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
Device# configure terminal | 

**Step 3**

ip ssh server algorithm hostkey
{x509v3-ssh-rsa [ssh-rsa] | ssh-rsa [x509v3-ssh-rsa]}

**Example:**
Device(config)# ip ssh server algorithm
hostkey x509v3-ssh-rsa

- Defines the order of host key algorithms. Only the configured algorithm is negotiated with the secure shell (SSH) client.

  **Note** The IOS SSH server must have at least one configured host key algorithm:
  - ssh-rsa – public key based authentication
  - x509v3-ssh-rsa – certificate-based authentication

**Step 4**

ip ssh server certificate profile

**Example:**
Device(config)# ip ssh server certificate profile

- Configures server certificate profile and user certificate profile and enters SSH certificate profile configuration mode.

**Step 5**

server

**Example:**
Device(ssh-server-cert-profile)# server

- Configures server certificate profile and enters SSH server certificate profile server configuration mode.

**Step 6**

trustpoint sign PKI-trustpoint-name

**Example:**
Device(ssh-server-cert-profile-server)# trustpoint sign trust1

- Attaches the public key infrastructure (PKI) trustpoint to the server certificate profile. The SSH server uses the certificate associated with this PKI trustpoint for server authentication.

**Step 7**

ocsp-response include

**Example:**
Device(ssh-server-cert-profile-server)# ocsp-response include

- (Optional) Sends the Online Certificate Status Protocol (OCSP) response or OCSP stapling along with the server certificate.

  **Note** By default the “no” form of this command is configured and no OCSP response is sent along with the server certificate.

**Step 8**

end

**Example:**
Device(ssh-server-cert-profile-server)# end

- Exits SSH server certificate profile server configuration mode and enters privileged EXEC mode.

---

**Configuring IOS SSH Server to Verify User’s Digital Certificate for User Authentication**

To configure IOS SSH Server to use digital certificates for user authentication, perform this procedure:
## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip ssh server algorithm authentication {publickey</td>
<td>keyboard</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ip ssh server algorithm authentication publickey</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The IOS SSH server must have at least one configured user authentication algorithm.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To use the certificate method for user authentication, the publickey keyword must be configured.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The <strong>ip ssh server algorithm authentication</strong> command replaces the <strong>ip ssh server authenticate user</strong> command.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip ssh server algorithm publickey {x509v3-ssh-rsa</td>
<td>ssh-rsa</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The IOS SSH client must have at least one configured public key algorithm:</td>
</tr>
<tr>
<td></td>
<td>• ssh-rsa – public-key-based authentication</td>
</tr>
<tr>
<td></td>
<td>• x509v3-ssh-rsa – certificate-based authentication</td>
</tr>
<tr>
<td><strong>Step 5</strong> ip ssh server certificate profile</td>
<td>Configures server certificate profile and enters SSH certificate profile configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ip ssh server certificate profile</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> user</td>
<td>Configures user certificate profile and enters SSH server certificate profile user configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(ssh-server-cert-profile)# user</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Step 7**

**trustpoint verify PKI-trustpoint-name**  
**Example:**  
Device(ssh-server-cert-profile-user)#  
trustpoint verify trust2

**Purpose**

Configures the public key infrastructure (PKI) trustpoint that is used to verify the incoming user certificate.  

**Note**

Configure multiple trustpoints by executing the same command multiple times. A maximum of 10 trustpoints can be configured.

**Step 8**

**ocsp-response required**  
**Example:**  
Device(ssh-server-cert-profile-user)#  
ocsp-response required

**Purpose**

(Optional) Mandates the presence of the Online Certificate Status Protocol (OCSP) response with the incoming user certificate.  

**Note**

By default the “no” form of this command is configured and the user certificate is accepted without an OCSP response.

**Step 9**

**end**  
**Example:**  
Device(ssh-server-cert-profile-user)#  
end

**Purpose**

Exits SSH server certificate profile user configuration mode and enters privileged EXEC mode.

## Verifying Configuration for Server and User Authentication Using Digital Certificates

To verify configuration for server and user Authentication using digital certificates, perform this procedure:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
**enable**  
**Example:**  
Device>enable | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2**
**show ip ssh**  
**Example:**  
Device#show ip ssh | Displays the currently configured authentication methods. To confirm the use of certificate-based authentication, ensure that the x509v3-ssh-rsa algorithm is the configured host key algorithm. |

**Example:**

Device# show ip ssh

SSH Enabled - version 1.99  
Authentication methods:publickey,keyboard-interactive,password  
Authentication Publickey  
Algorithms:x509v3-ssh-rsa,ssh-rsa  
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa  
Authentication timeout: 120 secs;  
Authentication retries: 3  
Minimum expected Diffie Hellman key size
### Configuration Examples for X.509v3 Certificates for SSH Authentication

The following section provides examples for user and server authentication using digital certificates.

#### Example: Configuring IOS SSH Server to Use Digital Certificates for Server Authentication

This example shows how to configure IOS SSH Server to Use Digital Certificates for Server Authentication.

```plaintext
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# server
Device(ssh-server-cert-profile-server)# trustpoint sign trust1
Device(ssh-server-cert-profile-server)# exit
```

#### Example: Configuring IOS SSH Server to Verify User's Digital Certificate for User Authentication

This example shows how to configure IOS SSH server to verify user's digital certificate for user authentication.

```plaintext
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm authentication publickey
Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# user
Device(ssh-server-cert-profile-user)# trustpoint verify trust2
Device(ssh-server-cert-profile-user)# end
```
Additional References for X.509v3 Certificates for SSH Authentication

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Security commands</td>
<td>• Cisco IOS Security Command Reference: Commands A to C</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands D to L</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands M to R</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands S to Z</td>
</tr>
<tr>
<td>SSH authentication</td>
<td>“Secure Shell-Configuring User Authentication Methods” chapter in Secure Shell Configuration Guide</td>
</tr>
<tr>
<td>Public key infrastructure (PKI) trustpoint</td>
<td>“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” chapter in Public Key Infrastructure Configuration Guide</td>
</tr>
</tbody>
</table>

Technical Assistance

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

Feature Information for X.509v3 Certificates for SSH Authentication

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

**Table 41: Feature Information for X.509v3 Certificates for SSH Authentication**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.509v3 Certificates for SSH Authentication</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>The X.509v3 Certificates for SSH Authentication feature uses the X.509v3 digital certificates in server and user authentication at the SSH server side.</td>
</tr>
</tbody>
</table>
CHAPTER 14

Configuring Secure Socket Layer HTTP

- Information about Secure Socket Layer HTTP, on page 241
- How to Configure Secure Socket Layer HTTP, on page 244
- Monitoring Secure HTTP Server and Client Status, on page 251
- Additional References for Secure Socket Layer HTTP, on page 251
- Feature Information for Secure Socket Layer HTTP, on page 252

Information about Secure Socket Layer 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://.

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 HTTPS server (or client) is automatically generated.

- If the switch is not configured with a hostname and a domain name, a temporary self-signed certificate is generated. If the switch reboots, any temporary self-signed certificate is lost, and a new temporary new self-signed certificate is assigned.

- If the switch has been configured with a host and domain name, a persistent self-signed certificate is generated. This certificate remains active if you reboot the switch or if you disable the secure HTTP server so that it will be there the next time you re-enable a secure HTTP connection.

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

When a new certificate is enrolled, the new configuration change is not applied to the HTTPS server until the server is restarted. You can restart the server using either the CLI or by physical reboot. On restarting the server, the switch starts using the new certificate.

If a self-signed certificate has been generated, this information is included in the output of the `show running-config` privileged EXEC command. This is a partial sample output from that command displaying a self-signed certificate.

```
Device# 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 00030201 02020101 30000609 2a864886 f70d0101 04050030
        39312f30 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 31330130 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.

---

**CipherSuites**

A CipherSuite specifies the encryption algorithm and the digest algorithm to use on a SSL connection. When connecting to the HTTPS server, the client Web browser offers a list of supported CipherSuites, and the client and server negotiate the best encryption algorithm to use from those on the list that are supported by both. For example, Netscape Communicator 4.76 supports U.S. security with RSA Public Key Cryptography, MD2, MD5, RC2-CBC, RC4, DES-CBC, and DES-EDE3-CBC.

For the best possible encryption, you should use a client browser that supports 128-bit encryption, such as Microsoft Internet Explorer Version 5.5 (or later) or Netscape Communicator Version 4.76 (or later). The SSL_RSA_WITH_DES_CBC_SHA CipherSuite provides less security than the other CipherSuites, as it does not offer 128-bit encryption.

The more secure and more complex CipherSuites require slightly more processing time. This list defines the CipherSuites supported by the switch and ranks them from fastest to slowest in terms of router processing load (speed):

1. SSL_RSA_WITH_DES_CBC_SHA—RSA key exchange (RSA Public Key Cryptography) with DES-CBC for message encryption and SHA for message digest
2. SSL_RSA_WITH_NULL_SHA key exchange with NULL for message encryption and SHA for message digest (only for SSL 3.0).
3. SSL_RSA_WITH_NULL_MD5 key exchange with NULL for message encryption and MD5 for message digest (only for SSL 3.0).
4. SSL_RSA_WITH_RC4_128_MD5—RSA key exchange with RC4 128-bit encryption and MD5 for message digest
5. SSL_RSA_WITH_RC4_128_SHA—RSA key exchange with RC4 128-bit encryption and SHA for message digest
6. SSL_RSA_WITH_3DES_EDE_CBC_SHA—RSA key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest
7. SSL_RSA_WITH_AES_128_CBC_SHA—RSA key exchange with AES 128-bit encryption and SHA for message digest (only for SSL 3.0).
8. SSL_RSA_WITH_AES_256_CBC_SHA—RSA key exchange with AES 256-bit encryption and SHA for message digest (only for SSL 3.0).
9. SSL_RSA_WITH_DHE_AES_128_CBC_SHA—RSA key exchange with AES 128-bit encryption and SHA for message digest (only for SSL 3.0).
10. SSL_RSA_WITH_DHE_AES_256_CBC_SHA—RSA key exchange with AES 256-bit encryption and SHA for message digest (only for SSL 3.0).

Note
The latest versions of Chrome do not support the four original cipher suites, thus disallowing access to both web GUI and guest portals.

RSA (in conjunction with the specified encryption and digest algorithm combinations) is used for both key generation and authentication on SSL connections. This usage is independent of whether or not a CA trustpoint is configured.

Default SSL Configuration

The standard HTTP server is enabled.
SSL is enabled.
No CA trustpoints are configured.
No self-signed certificates are generated.

SSL Configuration Guidelines

When SSL is used in a switch cluster, the SSL session terminates at the cluster commander. Cluster member switches must run standard HTTP.

Before you configure a CA trustpoint, you should ensure that the system clock is set. If the clock is not set, the certificate is rejected due to an incorrect date.

In a switch stack, the SSL session terminates at the stack master.

How to Configure Secure Socket Layer HTTP

Configuring a CA Trustpoint

For secure HTTP connections, we recommend that you configure an official CA trustpoint. A CA trustpoint is more secure than a self-signed certificate.

Beginning in privileged EXEC mode, follow these steps to configure a CA Trustpoint:

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Step 2** hostname hostname  
Example:  
Device(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 domain-name  
Example:  
Device(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:  
Device(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 name  
Example:  
Device(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 url  
Example:  
Device(ca-trustpoint)# enrollment url http://your_server:80 | Specifies the URL to which the switch should send certificate requests. |
| **Step 7** enrollment http-proxy host-name port-number  
Example:  
Device(ca-trustpoint)# enrollment http-proxy your_host 49 | (Optional) Configures the switch to obtain certificates from the CA through an HTTP proxy server.  
• For *host-name*, specify the proxy server used to get the CA.  
• For *port-number*, specify the port number used to access the CA. |
| **Step 8** crl query url  
Example:  
Device(ca-trustpoint)# crl query ldap://your_host:49 | Configures the switch to request a certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked. |
### Command or Action

**Step 9**
- **primary** `name`
  
  Example:
  
  Device(ca-trustpoint)# primary your_trustpoint

  *(Optional) Specifies that the trustpoint should be used as the primary (default) trustpoint for CA requests.*
  
  • For `name`, specify the trustpoint that you just configured.

**Step 10**
- **exit**
  
  Example:
  
  Device(ca-trustpoint)# exit

  *Exits CA trustpoint configuration mode and return to global configuration mode.*

**Step 11**
- **crypto ca authentication** `name`
  
  Example:
  
  Device(config)# crypto ca authentication your_trustpoint

  *Authenticates the CA by getting the public key of the CA. Use the same name used in Step 5.*

**Step 12**
- **crypto ca enroll** `name`
  
  Example:
  
  Device(config)# crypto ca enroll your_trustpoint

  *Obtains the certificate from the specified CA trustpoint. This command requests a signed certificate for each RSA key pair.*

**Step 13**
- **end**
  
  Example:
  
  Device(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:
AES256_SHA2 is not supported.

https://209.165.129:1026

or

https://host.domain.com:1026

The existing `ip http access-class access-list-number` command for specifying the access-list (Only IPv4 ACLs) is going to be deprecated. You can still use this command to specify an access list to allow access to the HTTP server. Two new commands have been introduced to enable support for specifying IPv4 and IPv6 ACLs. These are `ip http access-class ipv4 access-list-name | access-list-number` for specifying IPv4 ACLs and `ip http access-class ipv6 access-list-name` for specifying IPv6 ACLs. We recommend using the new CLI to avoid receiving warning messages.

Note the following considerations for specifying access-lists:

- If you specify an access-list that does not exist, the configuration takes place but you receive the below warning message:

  ACL being attached does not exist, please configure it

- If you use the `ip http access-class` command for specifying an access-list for the HTTP server, the below warning message appears:

  This CLI will be deprecated soon, Please use new CLI ip http access-class ipv4/ipv6 <access-list-name>|<access-list-number>

- If you use `ip http access-class ipv4 access-list-name | access-list-number` or `ip http access-class ipv6 access-list-name`, and an access-list was already configured using `ip http access-class`, the below warning message appears:

  Removing ip http access-class <access-list-number>

`ip http access-class access-list-number` and `ip http access-class ipv4 access-list-name | access-list-number` share the same functionality. Each command overrides the configuration of the previous command. The following combinations between the configuration of the two commands explain the effect on the running configuration:

- If `ip http access-class access-list-number` is already configured and you try to configure using `ip http access-class ipv4 access-list-number` command, the configuration of `ip http access-class access-list-number` will be removed and the configuration of `ip http access-class ipv4 access-list-number` will be added to the running configuration.

- If `ip http access-class access-list-number` is already configured and you try to configure using `ip http access-class ipv4 access-list-name` command, the configuration of `ip http access-class access-list-number` will be removed and the configuration of `ip http access-class ipv4 access-list-name` will be added to the running configuration.

- If `ip http access-class ipv4 access-list-number` is already configured and you try to configure using `ip http access-class access-list-name`, the configuration of `ip http access-class ipv4 access-list-number` will be removed from configuration and the configuration of `ip http access-class access-list-name` will be added to the running configuration.
- If `ip http access-class ipv4 access-list-name` is already configured and you try to configure using `ip http access-class access-list-number`, the configuration of `ip http access-class ipv4 access-list-name` will be removed from the configuration and the configuration of `ip http access-class access-list-number` will be added to the running configuration.

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>show ip http server status</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# show ip http server status</td>
<td>(Optional) Displays the status of the HTTP server to determine if the secure HTTP server feature is supported in the software. You should see one of these lines in the output:&lt;br&gt;HTTP secure server capability: Present or HTTP secure server capability: Not present</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>ip http secure-server</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)# ip http secure-server</td>
<td>Enables the HTTPS server if it has been disabled. The HTTPS server is enabled by default.</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>ip http secure-port</strong>&lt;br&gt;<strong>port-number</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)# ip http secure-port 443</td>
<td>(Optional) Specifies the port number to be used for the HTTPS server. The default port number is 443. Valid options are 443 or any number in the range 1025 to 65535.</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>ip http secure-ciphersuite</strong>&lt;br&gt;[[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]]&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)# ip http secure-ciphersuite rc4-128-md5</td>
<td>(Optional) Specifies the CipherSuites (encryption algorithms) to be used for encryption over the HTTPS connection. If you do not have a reason to specify a particularly CipherSuite, you should allow the server and client to negotiate a CipherSuite that they both support. This is the default.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 6    | ip http secure-client-auth  
**Example:**  
Device(config)# ip http secure-client-auth | (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. |
| 7    | ip http secure-trustpoint name  
**Example:**  
Device(config)# ip http secure-trustpoint your_trustpoint | 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. |
| 8    | ip http path path-name  
**Example:**  
Device(config)# ip http path /your_server:80 | (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). |
| 9    | ip http access-class access-list-number  
**Example:**  
Device(config)# ip http access-class 2 | (Optional) Specifies an access list to use to allow access to the HTTP server. |
| 10   | ip http access-class { ipv4  
{access-list-number | access-list-name}  
| ipv6 {access-list-name} }  
**Example:**  
Device(config)# ip http access-class ipv4 4 | (Optional) Specifies an access list to use to allow access to the HTTP server. |
| 11   | ip http max-connections value  
**Example:**  
Device(config)# ip http max-connections 4 | (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. |
| 12   | ip http timeout-policy idle seconds life requests value  
**Example:**  
Device(config)# ip http timeout-policy idle 120 life 240 requests 1 | (Optional) Specifies how long a connection to the HTTP server can remain open under the defined circumstances:  
•  **idle**—the maximum time period when no data is received or response data cannot |
### Configuring 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.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>(Optional) Specifies the CA trustpoint to be used if the remote HTTP server requests client authentication. Using this command assumes that you have already configured a CA trustpoint by using the previous procedure. The command is optional if client authentication is not needed or if a primary trustpoint has been configured.</td>
</tr>
<tr>
<td><code>ip http client secure-trustpoint name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# ip http client secure-trustpoint your_trustpoint</code></td>
<td></td>
</tr>
</tbody>
</table>

---

**Table:**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 13</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
Purpose

Command or Action | Purpose |
--- | --- |
Step 3 | (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. |

**Example:**

Device(config)# ip http client secure-ciphersuite rc4-128-md5

Step 4 | Returns to privileged EXEC mode. |

**Example:**

Device(config)# end

---

### 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 42: Commands for Displaying the SSL Secure Server and Client Status**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip http client secure status</td>
<td>Shows the HTTP secure client configuration.</td>
</tr>
<tr>
<td>show ip http server secure status</td>
<td>Shows the HTTP secure server configuration.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Shows the generated self-signed certificate for secure HTTP connections.</td>
</tr>
</tbody>
</table>

---

### Additional References for Secure Socket Layer HTTP

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Authority</td>
<td>Configuring Certification Authority Interoperability</td>
</tr>
</tbody>
</table>

**MIBs**

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

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

Feature Information for Secure Socket Layer HTTP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

<p>| Table 43: Feature Information for Secure Socket Layer HTTP |</p>
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Socket Layer HTTP</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>Cisco's implementation of the secure HTTP server and secure HTTP client uses an implementation of SSL Version 3.0 with application-layer encryption. On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet.</td>
</tr>
</tbody>
</table>
CHAPTER 15

IPv4 ACLs

- Information about Network Security with ACLs, on page 253
- Restrictions for Configuring IPv4 Access Control Lists, on page 253
- Understanding Network Security with ACLs, on page 255
- Supported ACLs, on page 255
- ACEs and Fragmented and Unfragmented Traffic, on page 258
- ACLs and Switch Stacks, on page 259
- Standard and Extended IPv4 ACLs, on page 260
- Hardware and Software Treatment of IP ACLs, on page 263
- VLAN Map Configuration Guidelines, on page 264
- VLAN Maps with Router ACLs, on page 264
- Time Ranges for ACLs, on page 265
- IPv4 ACL Interface Considerations, on page 266
- Information about Network Security with ACLs, on page 266
- How to Configure ACLs, on page 266
- Monitoring IPv4 ACLs, on page 284
- Configuration Examples for ACLs, on page 285
- IPv4 ACL Configuration Examples, on page 287
- Configuration Examples for ACLs and VLAN Maps, on page 292
- Configuration Examples for Using VLAN Maps in Your Network, on page 294
- Configuration Examples for ACLs, on page 296
- Feature Information for IPv4 ACLs, on page 296

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.

Restrictions for Configuring IPv4 Access Control Lists

General Network Security

The following are restrictions for configuring network security with ACLs:
• Not all commands that accept a numbered ACL accept a named ACL. ACLs for packet filters and route filters on interfaces can use a name. 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 wildcard is not supported in downstream client policy.

IPv4 ACL Network Interfaces

The following restrictions apply to IPv4 ACLs to network interfaces:

• When controlling access to an interface, you can use a named or numbered ACL.
• If you apply an ACL to a Layer 2 interface that is a member of a VLAN, the Layer 2 (port) ACL takes precedence over an input Layer 3 ACL applied to the VLAN interface or a VLAN map applied to the VLAN.
• If you apply an ACL to a Layer 3 interface and routing is not enabled on the switch, the ACL only filters packets that are intended for the CPU, such as SNMP, Telnet, or web traffic.
• If the `preauth_ipv4_acl` ACL is configured to filter packets, the ACL is removed after authentication.
• You do not have to enable routing to apply ACLs to Layer 2 interfaces.

MAC ACLs on a Layer 2 Interface

After you create a MAC ACL, you can apply it to a Layer 2 interface to filter non-IP traffic coming in that interface. When you apply the MAC ACL, consider these guidelines:

• You can apply no more than one IP access list and one MAC access list to the same Layer 2 interface. The IP access list filters only IP packets, and the MAC access list filters non-IP packets.
• A Layer 2 interface can have only one MAC access list. If you apply a MAC access list to a Layer 2 interface that has a MAC ACL configured, the new ACL replaces the previously configured one.

Note

The `mac access-group` interface configuration command is only valid when applied to a physical Layer 2 interface. You cannot use the command on EtherChannel port channels.

IP Access List Entry Sequence Numbering

• This feature does not support dynamic, reflexive, or firewall access lists.
Understanding Network Security with ACLs

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:

- Port ACLs access-control traffic entering a Layer 2 interface. You can apply port ACLs to a Layer 2 interface in each direction to each access list type — IPv4 and MAC.

- Router ACLs access-control routed traffic between VLANs and are applied to Layer 3 interfaces in a specific direction (inbound or outbound).
ACL Precedence

When Port ACLs, and router ACLs are configured on the same switch, the filtering precedence, from greatest to least for ingress traffic is port ACL, and then router ACL. For egress traffic, the filtering precedence is router ACL, and then port ACL.

The following examples describe simple use cases:

- 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.

Port ACLs

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

The switch examines ACLs on an interface and permits or denies packet forwarding based on how the packet matches the entries in the ACL. In this way, ACLs control access to a network or to part of a network.

Figure 15: Using ACLs to Control Traffic in a Network

This is an example of using port ACLs to control access to a network when all workstations are in the same VLAN. ACLs applied at the Layer 2 input would allow Host A to access the Human Resources network, but prevent Host B from accessing the same network. Port ACLs can only be applied to Layer 2 interfaces in the inbound direction.

When you apply a port ACL to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. When you apply a port ACL to a port with voice VLAN, the ACL filters traffic on both data and voice VLANs.
With port ACLs, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC addresses. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP access list and a MAC access list to the interface.

**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.

The switch supports these access lists for IPv4 traffic:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses and optional protocol type information for matching operations.

As with port ACLs, the switch examines ACLs associated with features configured on a given interface. As packets enter the switch on an interface, ACLs associated with all inbound features configured on that interface are examined. After packets are routed and before they are forwarded to the next hop, all ACLs associated with outbound features configured on the egress interface are examined.

ACLs permit or deny packet forwarding based on how the packet matches the entries in the ACL, and can be used to control access to a network or to part of a network.

**VLAN Maps**

VLAN ACLs or VLAN maps are used to control network traffic within a VLAN. You can apply VLAN maps to all packets that are bridged within a VLAN in the switch or switch stack. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VACLs are not defined by direction (ingress or egress).

All non-IP protocols are access-controlled through MAC addresses and Ethertype using MAC VLAN maps. (IP traffic is not access controlled by MAC VLAN maps.) You can enforce VLAN maps only on packets going through the switch; you cannot enforce VLAN maps on traffic between hosts on a hub or on another switch connected to this switch.

With VLAN maps, forwarding of packets is permitted or denied, based on the action specified in the map.
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.

For TCP ACEs with L4 Ops, the fragmented packets will be dropped per RFC 1858.

- Deny ACEs that check Layer 4 information never match a fragment unless the fragment contains Layer 4 information.

ACEs and Fragmented and Unfragmented Traffic Examples

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

```
Device(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Device(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Device(config)# access-list 102 permit tcp any host 10.1.1.2
Device(config)# access-list 102 deny tcp any any
```

In the first and second ACEs in the examples, the `eq` keyword after the destination address means to test for the TCP-destination-port well-known numbers equaling Simple Mail Transfer Protocol (SMTP) and Telnet, respectively.
• Packet A is a TCP packet from host 10.2.2.2., port 65000, going to host 10.1.1.1 on the SMTP port. If this packet is fragmented, the first fragment matches the first ACE (a permit) as if it were a complete packet because all Layer 4 information is present. The remaining fragments also match the first ACE, even though they do not contain the SMTP port information, because the first ACE only checks Layer 3 information when applied to fragments. The information in this example is that the packet is TCP and that the destination is 10.1.1.1.

• Packet B is from host 10.2.2.2, port 65001, going to host 10.1.1.2 on the Telnet port. If this packet is fragmented, the first fragment matches the second ACE (a deny) because all Layer 3 and Layer 4 information is present. The remaining fragments in the packet do not match the second ACE because they are missing Layer 4 information. Instead, they match the third ACE (a permit). Because the first fragment was denied, host 10.1.1.2 cannot reassemble a complete packet, so packet B is effectively denied. However, the later fragments that are permitted will consume bandwidth on the network and resources of host 10.1.1.2 as it tries to reassemble the packet.

• Fragmented packet C is from host 10.2.2.2, port 65001, going to host 10.1.1.3, port ftp. If this packet is fragmented, the first fragment matches the fourth ACE (a deny). All other fragments also match the fourth ACE because that ACE does not check any Layer 4 information and because Layer 3 information in all fragments shows that they are being sent to host 10.1.1.3, and the earlier permit ACEs were checking different hosts.

### ACLs and Switch Stacks

ACL support is the same for a switch stack as for a standalone switch. ACL configuration information is propagated to all switches in the stack. All switches in the stack, including the active switch, process the information and program their hardware.

### Active Switch and ACL Functions

The active switch performs these ACL functions:

• It processes the ACL configuration and propagates the information to all stack members.

• It distributes the ACL information to any switch that joins the stack.

• If packets must be forwarded by software for any reason (for example, not enough hardware resources), the active switch forwards the packets only after applying ACLs on the packets.

• It programs its hardware with the ACL information it processes.

### Stack Member and ACL Functions

Stack members perform these ACL functions:

• They receive the ACL information from the active switch and program their hardware.

• A stack member configured as a standby switch, performs the functions of the active switch in the event the active switch fails.
Active Switch Failure and ACLs

Both the active and standby switches have the ACL information. When the active switch fails, the standby takes over. The new active switch distributes the ACL information to all stack members.

Standard and Extended IPv4 ACLs

This section describes IP ACLs.

An ACL is a sequential collection of permit and deny conditions. One by one, the switch tests packets against the conditions in an access list. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing after the first match, the order of the conditions is critical. If no conditions match, the switch denies the packet.

The software supports these types of ACLs or access lists for IPv4:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses for matching operations and optional protocol-type information for finer granularity of control.

IPv4 ACL Switch Unsupported Features

Configuring IPv4 ACLs on the switch is the same as configuring IPv4 ACLs on other Cisco switches and routers.

The following ACL-related features are not supported:

- Non-IP protocol ACLs
- IP accounting
- Reflexive ACLs and dynamic ACLs are not supported.

Access List Numbers

The number you use to denote your ACL shows the type of access list that you are creating.

This lists the access-list number and corresponding access list type and shows whether or not they are supported in the switch. The switch supports IPv4 standard and extended access lists, numbers 1 to 199 and 1300 to 2699.

Table 44: Access List Numbers

<table>
<thead>
<tr>
<th>Access List Number</th>
<th>Type</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>1–99</td>
<td>IP standard access list</td>
<td>Yes</td>
</tr>
<tr>
<td>100–199</td>
<td>IP extended access list</td>
<td>Yes</td>
</tr>
<tr>
<td>200–299</td>
<td>Protocol type-code access list</td>
<td>No</td>
</tr>
<tr>
<td>300–399</td>
<td>DECnet access list</td>
<td>No</td>
</tr>
</tbody>
</table>
Numbered Standard IPv4 ACLs

When creating an ACL, remember that, by default, the end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end. With standard access lists, if you omit the mask from an associated IP host address ACL specification, 0.0.0.0 is assumed to be the mask.

The switch always rewrites the order of standard access lists so that entries with host matches and entries with matches having a don’t care mask of 0.0.0.0 are moved to the top of the list, above any entries with non-zero don’t care masks. Therefore, in show command output and in the configuration file, the ACEs do not necessarily appear in the order in which they were entered.

After creating a numbered standard IPv4 ACL, you can apply it to , 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 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.
**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**

ACL logging is only supported for RACL.

---

**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.

---

**Note**

The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

---

**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.

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

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

When you enter the `show ip access-lists` privileged EXEC command, the match count displayed does not account for packets that are access controlled in hardware. Use the `show platform software fed switch { switch_num | active | standby } acl counters hardware` privileged EXEC command to obtain some basic hardware ACL statistics for switched and routed packets.

Router ACLs function as follows:
• The hardware controls permit and deny actions of standard and extended ACLs (input and output) for security access control.

• If log has not been specified, the flows that match a deny statement in a security ACL are dropped by the hardware if ip unreachables is disabled. The flows matching a permit statement are switched in hardware.

• Adding the log keyword to an ACE in a router ACL causes a copy of the packet to be sent to the CPU for logging only. If the ACE is a permit statement, the packet is still switched and routed in hardware.

VLAN Map Configuration Guidelines

VLAN maps are the only way to control filtering within a VLAN. VLAN maps have no direction. To filter traffic in a specific direction by using a VLAN map, you need to include an ACL with specific source or destination addresses. If there is a match clause for that type of packet (IP or MAC) in the VLAN map, the default action is to drop the packet if the packet does not match any of the entries within the map. If there is no match clause for that type of packet, the default is to forward the packet.

The following are the VLAN map configuration guidelines:

• If there is no ACL configured to deny traffic on an interface and no VLAN map is configured, all traffic is permitted.

• Each VLAN map consists of a series of entries. The order of entries in an VLAN map is important. A packet that comes into the switch is tested against the first entry in the VLAN map. If it matches, the action specified for that part of the VLAN map is taken. If there is no match, the packet is tested against the next entry in the map.

• If the VLAN map has at least one match clause for the type of packet (IP or MAC) and the packet does not match any of these match clauses, the default is to drop the packet. If there is no match clause for that type of packet in the VLAN map, the default is to forward the packet.

• Logging is not supported for VLAN maps.

• When a switch has an IP access list or MAC access list applied to a Layer 2 interface, and you apply a VLAN map to a VLAN that the port belongs to, the port ACL takes precedence over the VLAN map.

• If a VLAN map configuration cannot be applied in hardware, all packets in that VLAN are dropped.

VLAN Maps with Router ACLs

To access control both bridged and routed traffic, you can use VLAN maps only or a combination of router ACLs and VLAN maps. You can define router ACLs on both input and output routed VLAN interfaces, and you can define a VLAN map to access control the bridged traffic.

If a packet flow matches a VLAN-map deny clause in the ACL, regardless of the router ACL configuration, the packet flow is denied.

Note

When you use router ACLs with VLAN maps, packets that require logging on the router ACLs are not logged if they are denied by a VLAN map.
If the VLAN map has a match clause for the type of packet (IP or MAC) and the packet does not match the type, the default is to drop the packet. If there is no match clause in the VLAN map, and no action specified, the packet is forwarded if it does not match any VLAN map entry.

**VLAN Maps and Router ACL Configuration Guidelines**

These guidelines are for configurations where you need to have an router ACL and a VLAN map on the same VLAN. These guidelines do not apply to configurations where you are mapping router ACLs and VLAN maps on different VLANs.

If you must configure a router ACL and a VLAN map on the same VLAN, use these guidelines for both router ACL and VLAN map configuration:

- You can configure only one VLAN map and one router ACL in each direction (input/output) on a VLAN interface.
- Whenever possible, try to write the ACL with all entries having a single action except for the final, default action of the other type. That is, write the ACL using one of these two forms:
  
  ```
  permit... permit... permit... deny ip any any
  ```
  
  ```
  deny... deny... deny... permit ip any any
  ```

- To define multiple actions in an ACL (permit, deny), group each action type together to reduce the number of entries.
- Avoid including Layer 4 information in an ACL; adding this information complicates the merging process. The best merge results are obtained if the ACLs are filtered based on IP addresses (source and destination) and not on the full flow (source IP address, destination IP address, protocol, and protocol ports). It is also helpful to use *don’t care* bits in the IP address, whenever possible.

If you need to specify the full-flow mode and the ACL contains both IP ACEs and TCP/UDP/ICMP ACEs with Layer 4 information, put the Layer 4 ACEs at the end of the list. This gives priority to the filtering of traffic based on IP addresses.

**Time Ranges for ACLs**

You can selectively apply extended ACLs based on the time of day and the week by using the `time-range` global configuration command. First, define a time-range name and set the times and the dates or the days of the week in the time range. Then enter the time-range name when applying an ACL to set restrictions to the access list. You can use the time range to define when the permit or deny statements in the ACL are in effect, for example, during a specified time period or on specified days of the week. The `time-range` keyword and argument are referenced in the named and numbered extended ACL task tables.

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.)
The timer range relies on the switch system clock; therefore, you need a reliable clock source. We recommend that you use Network Time Protocol (NTP) to synchronize the switch clock.

### IPv4 ACL Interface Considerations

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.

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.

### 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.

### How to Configure ACLs

#### Configuring IPv4 ACLs

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

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create an ACL by specifying an access list number or name and the access conditions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Apply the ACL to interfaces or terminal lines. You can also apply standard and extended IP ACLs to VLAN maps.</td>
</tr>
</tbody>
</table>

#### Creating a Numbered Standard ACL

Follow these steps to create a numbered standard ACL:
## IPv4 ACLs

### Creating a Numbered Standard ACL

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device&gt; <strong>enable</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# <strong>configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>access-list</strong> access-list-number {deny</td>
<td>permit} source source-wildcard</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# <strong>access-list</strong> 2 deny your_host</td>
<td>The access-list-number 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 source is the source address of the network or host from which the packet is being sent specified as:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The 32-bit quantity in dotted-decimal format.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The keyword any as an abbreviation for source and source-wildcard of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The keyword host as an abbreviation for source and source-wildcard of source 0.0.0.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional) The source-wildcard applies wildcard bits to the source.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Logging is supported only on ACLs attached to Layer 3 interfaces.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# <strong>end</strong></td>
<td></td>
</tr>
</tbody>
</table>
Creating a Numbered Extended ACL

Follow these steps to create a numbered extended ACL:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> access-list access-list-number {deny</td>
<td>permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]</td>
</tr>
<tr>
<td>Example: Device(config)# access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log</td>
<td></td>
</tr>
</tbody>
</table>

This step includes options for most IP protocols. For additional specific parameters for TCP, UDP, ICMP, and IGMP, see the following steps.

---

*Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)*
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>The source is the number of the network or host from which the packet is sent. The source-wildcard applies wildcard bits to the source. The destination is the network or host number to which the packet is sent. The destination-wildcard applies wildcard bits to the destination. Source, source-wildcard, destination, and destination-wildcard can be specified as:</td>
<td></td>
</tr>
<tr>
<td>• The 32-bit quantity in dotted-decimal format.</td>
<td>• The keyword any for 0.0.0.0 255.255.255.255 (any host).</td>
</tr>
<tr>
<td>• The keyword host for a single host 0.0.0.0.</td>
<td>• The other keywords are optional and have these meanings:</td>
</tr>
<tr>
<td>• 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).</td>
<td>• fragments—Enter to check non-initial fragments.</td>
</tr>
<tr>
<td>• 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).</td>
<td>• time-range—Specify the time-range name.</td>
</tr>
<tr>
<td>• dscp—Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values.</td>
<td>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.</td>
</tr>
</tbody>
</table>
### IPv4 ACLs

#### Creating a Numbered Extended ACL

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list access-list-number {deny</td>
<td>permit} tcp source source-wildcard [operator port] destination destination-wildcard [operator port] [established] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp] [flag]</td>
<td>Defines an extended TCP access list and the access conditions. The parameters are the same as those described for an extended IPv4 ACL, with these exceptions: (Optional) Enter an operator and port to compare source (if positioned after source source-wildcard) or destination (if positioned after destination destination-wildcard) port. Possible operators include eq (equal), gt (greater than), lt (less than), neq (not equal), and range (inclusive range). Operators require a port number (range requires two port numbers separated by a space). Enter the port number as a decimal number (from 0 to 65535) or the name of a TCP port. Use only TCP port numbers or names when filtering TCP. The other optional keywords have these meanings: • established—Enter to match an established connection. This has the same function as matching on the ack or rst flag. • flag—Enter one of these flags to match by the specified TCP header bits: ack (acknowledge), fin (finish), psh (push), rst (reset), syn (synchronize), or urg (urgent).</td>
</tr>
</tbody>
</table>

Example:

```
Device(config)# access-list 101 permit tcp any any eq 500
```

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list access-list-number {deny</td>
<td>permit} udp source source-wildcard [operator port] destination destination-wildcard [operator port] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]</td>
<td>(Optional) Defines an extended UDP access list and the access conditions. The UDP parameters are the same as those described for TCP except that the [operator [port]] port number or name must be a UDP port number or name, and the flag and established keywords are not valid for UDP.</td>
</tr>
</tbody>
</table>

Example:

```
Device(config)# access-list 101 permit udp any any eq 100
```

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list access-list-number {deny</td>
<td>permit} icmp source source-wildcard destination destination-wildcard [icmp-type [[icmp-type [icmp-code] [icmp-message] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]]]]</td>
<td>Defines an extended ICMP access list and the access conditions. The ICMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with the addition of the ICMP</td>
</tr>
</tbody>
</table>
## Purpose

Command or Action

Example:

```
Device(config)# access-list 101 permit icmp any any 200
```

Purpose

message type and code parameters. These optional keywords have these meanings:

- **icmp-type**—Enter to filter by ICMP message type, a number from 0 to 255.
- **icmp-code**—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255.
- **icmp-message**—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name.

### Step 6

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `access-list access-list-number {deny | permit} igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]` | (Optional) Defines an extended IGMP access list and the access conditions. The IGMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with this optional parameter. **igmp-type**—To match IGMP message type, enter a number from 0 to 15, or enter the message name: `dvmrp`, `host-query`, `host-report`, `pim`, or `trace`.

Example:

```
Device(config)# access-list 101 permit igmp any any 14
```

### Step 7

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `end` | Returns to privileged EXEC mode.

Example:

```
Device(config)# end
```

---

## Creating Named Standard ACLs

Follow these steps to create a standard ACL using names:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
</tbody>
</table>

Example:

```
Device> enable
```

| **Step 2** configure terminal | Enters global configuration mode. |

Example:
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>ip access-list standard name</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip access-list standard 20</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Use one of the following:</td>
</tr>
<tr>
<td>• deny {source [source-wildcard]</td>
<td>host source</td>
</tr>
<tr>
<td>• permit {source [source-wildcard]</td>
<td>host source</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255 or Device(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-std-nacl)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>show running-config</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
## Creating Extended Named ACLs

Follow these steps to create an extended ACL using names:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ip access-list extended name</code></td>
<td>Defines an extended IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 100 to 199.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# ip access-list extended 150</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`{deny</td>
<td>permit} protocol {source [source-wildcard]</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-ext-nacl)# permit 0 any any</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-ext-nacl)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> time-range time-range-name</td>
<td>Assigns a meaningful name (for example, <code>workhours</code>) to the time range to be created, and enter time-range configuration mode. The name cannot contain a space or quotation mark and must begin with a letter.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# time-range workhours</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Use one of the following:</td>
</tr>
<tr>
<td></td>
<td>• absolute [start time date] [end time date]</td>
</tr>
<tr>
<td></td>
<td>• periodic day-of-the-week hh:mm to [day-of-the-week] hh:mm</td>
</tr>
<tr>
<td></td>
<td>• periodic {weekdays</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>Device(config-time-range)# periodic weekdays 8:00 to 12:00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 5</strong></th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config)# end</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 6</strong></th>
<th>show running-config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device# show running-config</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 7</strong></th>
<th>copy running-config startup-config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device# copy running-config startup-config</td>
</tr>
</tbody>
</table>

**What to do next**
Repeat the steps if you have multiple items that you want in effect at different times.

**Applying an IPv4 ACL to a Terminal Line**

You can use numbered ACLs to control access to one or more terminal lines. You cannot apply named ACLs to lines. You must set identical restrictions on all the virtual terminal lines because a user can attempt to connect to any of them.

Follow these steps to restrict incoming and outgoing connections between a virtual terminal line and the addresses in an ACL:
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> line [console</td>
<td>vty] line-number</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# line console 0</td>
<td></td>
</tr>
<tr>
<td>* console — Specifies the console terminal line. The console port is DCE.</td>
<td></td>
</tr>
<tr>
<td>* vty — Specifies a virtual terminal for remote console access.</td>
<td></td>
</tr>
<tr>
<td>The line-number 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> access-class access-list-number {in</td>
<td>out}</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-line)# access-class 10 in</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-line)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# copy running-config</td>
<td></td>
</tr>
</tbody>
</table>
Applying an IPv4 ACL to an Interface

This section describes how to apply IPv4 ACLs to network interfaces.

Beginning in privileged EXEC mode, follow these steps to control access to an interface:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Identifies a specific interface for configuration, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>The interface can be a Layer 2 interface (port ACL), or a Layer 3 interface (router ACL).</td>
</tr>
<tr>
<td></td>
<td>Device(config)# interface gigabitethernet1/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip access-group {access-list-number</td>
<td>name} {in</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# ip access-group 2 in</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
<td>Displays the access list configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# copy running-config</td>
<td></td>
</tr>
</tbody>
</table>
Creating Named MAC Extended ACLs

You can filter non-IPv4 traffic on a VLAN or on a Layer 2 interface by using MAC addresses and named MAC extended ACLs. The procedure is similar to that of configuring other extended named ACLs.

Follow these steps to create a named MAC extended ACL:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

### Step 1

Enables privileged EXEC mode. Enters global configuration mode.

**Example:**

```
Device> enable
```

### Step 2

Enters global configuration mode.

**Example:**

```
Device# configure terminal
```

### Step 3

Defines an extended MAC access list using a name.

**Example:**

```
Device(config)# mac access-list extended mac1
```

### Step 4

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:

- `type mask`—An arbitrary EtherType number of a packet with Ethernet II or SNAP encapsulation in decimal, hexadecimal, or octal with optional mask of `don’t care` bits applied to the EtherType before testing for a match.

**Example:**

```
Device(config-ext-macl)# deny any any deenet-iv
```

or

```
Device(config-ext-macl)# deny any any deenet-iv 00-00-00-00-00-00
```
Applying a MAC ACL to a Layer 2 Interface

Follow these steps to apply a MAC access list to control access to a Layer 2 interface:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

### Command: Device(config-ext-macl)##

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit any any</td>
<td>Applies an ACL entry to control access.</td>
</tr>
</tbody>
</table>

### Examples

**Step 5**

Device(config-ext-macl)# end

Example:

Returns to privileged EXEC mode.

**Step 6**

Device# show running-config

Example:

Verifies your entries.

**Step 7**

Device# copy running-config startup-config

Example:

(Optional) Saves your entries in the configuration file.

---

IPv4 ACLs

### Applying a MAC ACL to a Layer 2 Interface

Follow these steps to apply a MAC access list to control access to a Layer 2 interface:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

### Command: Device(config-ext-macl)##

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit any any</td>
<td>Applies an ACL entry to control access.</td>
</tr>
</tbody>
</table>

### Examples

**Step 5**

Device(config-ext-macl)# end

Example:

Returns to privileged EXEC mode.

**Step 6**

Device# show running-config

Example:

Verifies your entries.

**Step 7**

Device# copy running-config startup-config

Example:

(Optional) Saves your entries in the configuration file.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td><code>interface interface-id</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# interface gigabitethernet1/0/2</td>
<td>Identifies a specific interface, and enter interface configuration mode. The interface must be a physical Layer 2 interface (port ACL).</td>
</tr>
<tr>
<td>4</td>
<td><code>mac access-group {name} {in }</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-if)# mac access-group mac1 in</td>
<td>Controls access to the specified interface by using the MAC access list. Port ACLs are supported in the inbound directions.</td>
</tr>
<tr>
<td>5</td>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-if)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td><code>show mac access-group [interface interface-id]</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: Device# show mac access-group interface gigabitethernet1/0/2</td>
<td>Displays the MAC access list applied to the interface or all Layer 2 interfaces.</td>
</tr>
<tr>
<td>7</td>
<td><code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: Device# show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>8</td>
<td><code>copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: Device# copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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.

# Configuring VLAN Maps

To create a VLAN map and apply it to one or more VLANs, perform these steps:

**Before you begin**

Create the standard or extended IPv4 ACLs or named MAC extended ACLs that you want to apply to the VLAN.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Creates a VLAN map, and give it a name and (optionally) a number. The number is the sequence number of the entry within the map.</td>
</tr>
<tr>
<td><code>vlan access-map name [number]</code></td>
<td>When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete. 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. Entering this command changes to access-map configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Device(config)# vlan access-map map_1 20</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | 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. **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. |
| `match {ip | mac} address {name | number} [name | number]` | |
| Example: `Device(config-access-map)# match ip address ip2` | |
### Creating a VLAN Map

Each VLAN map consists of an ordered series of entries. Beginning in privileged EXEC mode, follow these steps to create, add to, or delete a VLAN map entry:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Creates a VLAN map, and give it a name and (optionally) a number. The number is the sequence number of the entry within the map.</td>
</tr>
<tr>
<td><code>vlan access-map name [number]</code></td>
<td>When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete.</td>
</tr>
</tbody>
</table>

### Command or Action

- **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):
  - `action { forward }

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

  - `action { drop }

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

- **Step 4** `vlan filter mapname vlan-list list`

  **Example:**

  ```
  Device(config)# vlan filter map 1 vlan-list 20-22
  ```

  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.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VLAN maps do not use the specific permit or deny keywords. To deny a packet by using VLAN maps, create an ACL that would match the packet, and set the action to drop. A permit in the ACL counts as a match. A deny in the ACL means no match. Enterling this command changes to access-map configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>match {ip</td>
</tr>
<tr>
<td>Example:</td>
<td>Match the packet (using either the IP or MAC address) against one or more standard or extended access lists. Note that packets are only matched against access lists of the correct protocol type. IP packets are matched against standard or extended IP access lists. Non-IP packets are only matched against named MAC extended access lists.</td>
</tr>
<tr>
<td>Step 4</td>
<td>action {drop</td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Sets the action for the map entry. The default is to forward.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show running-config</td>
</tr>
<tr>
<td>Example:</td>
<td>Displays the access list configuration.</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**Applying a VLAN Map to a VLAN**

Beginning in privileged EXEC mode, follow these steps to apply a VLAN map to one or more VLANs:
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Applies the VLAN map to one or more VLAN IDs.</td>
</tr>
<tr>
<td><code>vlan filter mapname vlan-list list</code></td>
<td>The list can be a single VLAN ID (22), a consecutive list (10-22), or a string of VLAN IDs (12, 22, 30). Spaces around the comma and hyphen are optional.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# vlan filter map 1 vlan-list 20-22</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Displays the access list configuration.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show running-config</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# copy running-config startup-config</td>
</tr>
</tbody>
</table>

### 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 45: Commands for Displaying Access Lists and Access Groups

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show access-lists [number</td>
<td>name]`</td>
</tr>
<tr>
<td>`show ip access-lists [number</td>
<td>name]`</td>
</tr>
<tr>
<td><code>show ip interface interface-id</code></td>
<td>Displays detailed configuration and status of an interface. If IP is enabled on the interface and ACLs have been applied by using the <code>ip access-group</code> interface configuration command, the access groups are included in the display.</td>
</tr>
<tr>
<td><code>show running-config [interface interface-id]</code></td>
<td>Displays the contents of the configuration file for the switch or the specified interface, including all configured MAC and IP access lists and which access groups are applied to an interface.</td>
</tr>
<tr>
<td><code>show mac access-group [interface interface-id]</code></td>
<td>Displays MAC access lists applied to all Layer 2 interfaces or the specified Layer 2 interface.</td>
</tr>
</tbody>
</table>

### Configuration Examples for ACLs

#### Examples: Using Time Ranges with ACLs

This example shows how to verify after you configure time ranges for `workhours` and to configure January 1, 2006, as a company holiday.

```
Device# show time-range
time-range entry: new_year_day_2003 (inactive)
  absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
  periodic weekdays 8:00 to 12:00
  periodic weekdays 13:00 to 17:00
```

To apply a time range, enter the time-range name in an extended ACL that can implement time ranges. This example shows how to create and verify extended access list 188 that denies TCP traffic from any source to any destination during the defined holiday times and permits all TCP traffic during work hours.

```
Device(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Device(config)# access-list 188 permit tcp any any time-range workhours
```
This example uses named ACLs to permit and deny the same traffic.

```
Device(config)# ip access-list extended deny_access
Device(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Device(config-ext-nacl)# exit
Device(config)# ip access-list extended may_access
Device(config-ext-nacl)# permit tcp any any time-range workhours
Device(config-ext-nacl)# end
Device(config)# 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` 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:

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

```
Device(config)# ip access-list extended telnetting
Device(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Device(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```
IPv4 ACL Configuration Examples

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.

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.

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

Device(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Device(config)# end
Device# show access-lists
Extended IP access list 106
  10 permit ip any 172.20.128.64 0.0.0.31
Device(config)# interface gigabitethernet1/0/1
Device(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.

Device(config)# access-list 2 permit 36.48.0.3
Device(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Device(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Device(config)# interface gigabitethernet2/0/1
Device(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.

Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Device(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Device(config)# access-list 102 permit icmp any any
Device(config)# interface gigabitethernet2/0/1
Device(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. Because the secure system of the network always accepts mail connections on port 25, the incoming are separately controlled.
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
Device(config)# interface gigabitethernet1/0/1
Device(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.

Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Device(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Device(config)# interface gigabitethernet1/0/1
Device(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.

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

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

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

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

```
Device(config)# time-range no-http
Device(config)# periodic weekdays 8:00 to 18:00

Device(config)# time-range udp-yes
Device(config)# periodic weekend 12:00 to 20:00

Device(config)# ip access-list extended strict
Device(config-ext-nacl)# deny tcp any any eq www time-range no-http
Device(config-ext-nacl)# permit udp any any time-range udp-yes

Device(config-ext-nacl)# exit
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# ip access-group strict in
```

Examples: Configuring Commented IP ACL Entries

In this example of a numbered ACL, the workstation that belongs to Jones is allowed access, and the workstation that belongs to Smith is not allowed access:

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

```
Device(config)# access-list 100 remark Do not allow Winter to browse the web
Device(config)# access-list 100 deny host 171.69.3.85 any eq www
Device(config)# access-list 100 remark Do not allow Smith to browse the web
Device(config)# access-list 100 deny host 171.69.3.13 any eq www
```

In this example of a named ACL, the Jonessubnet is not allowed access:

```
Device(config)# ip access-list standard prevention
Device(config-std-nacl)# remark Do not allow Jones subnet through
Device(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

In this example of a named ACL, the Jonessubnet is not allowed to use outbound 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.

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

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.

```
Device(config)# ip access-list extended ext1
Device(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Device(config-ext-nacl)# deny udp any any log
Device(config-ext-nacl)# exit
Device(config)# interface gigabitethernet1/0/2
Device(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-IPACCESSLOGDP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(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.

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

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

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

Device(config-ext-nacl)# permit tcp any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map drop-ip-default 10
Device(config-access-map)# match ip address 101
Device(config-access-map)# action forward
Device(config-access-map)# exit
Device(config)# vlan access-map drop-ip-default 20
Device(config-access-map)# match ip address igmp-match
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(config)# vlan access-map drop-ip-default 30
Device(config-access-map)# match ip address tcp-match
Device(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

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

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

Configuration Examples for Using VLAN Maps in Your Network

Example: Wiring Closet Configuration

Figure 18: Wiring Closet Configuration

In a wiring closet configuration, routing might not be enabled on the switch. In this configuration, the switch can still support a VLAN map and a QoS classification ACL. Assume that Host X and Host Y are in different VLANs and are connected to wiring closet switches A and C. Traffic from Host X to Host Y is eventually being routed by Switch B, a Layer 3 switch with routing enabled. Traffic from Host X to Host Y can be access-controlled at the traffic entry point, Switch A.

If you do not want HTTP traffic switched from Host X to Host Y, you can configure a VLAN map on Switch A to drop all HTTP traffic from Host X (IP address 10.1.1.32) to Host Y (IP address 10.1.1.34) at Switch A and not bridge it to Switch B.

First, define the IP access list http that permits (matches) any TCP traffic on the HTTP port.
Device(config)# ip access-list extended http
Device(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Device(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.

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

Then, apply VLAN access map map2 to VLAN 1.

Device(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.
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 SERVER 1 that denies access to hosts in subnet 10.1.2.0, 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.

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

```
Device(config)# vlan access-map SERVER1_MAP
Device(config-access-map)# match ip address SERVER1_ACL
Device(config-access-map)# action drop
Device(config)# vlan access-map SERVER1_MAP 20
Device(config-access-map)# action forward
Device(config-access-map)# exit
```

Apply the VLAN map to VLAN 10.

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

Configuration Examples for ACLs

Feature Information for IPv4 ACLs

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

```
Table 46: Feature Information for IPv4 ACLs

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 ACLs</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This chapter describes how to configure network security on the switch by using ACLs. 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.</td>
</tr>
</tbody>
</table>
```
IPv6 ACLs Overview

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

A switch supports three types of IPv6 ACLs:

- IPv6 router ACLs are supported on outbound or inbound traffic on Layer 3 interfaces, which can be routed ports, switch virtual interfaces (SVIs), or Layer 3 EtherChannels. IPv6 router ACLs apply only to IPv6 packets that are routed.

- IPv6 port ACLs are supported on outbound and inbound Layer 2 interfaces. IPv6 port ACLs are applied to all IPv6 packets entering the interface.

- VLAN ACLs or VLAN maps access-control all packets in a VLAN. You can use VLAN maps to filter traffic between devices in the same VLAN. ACL VLAN maps are applied on L2 VLANs. VLAN maps are configured to provide access control based on Layer 3 addresses for IPv6. Unsupported protocols are access-controlled through MAC addresses using Ethernet ACEs. After a VLAN map is applied to a VLAN, all packets entering the VLAN are checked against the VLAN map.

The switch supports VLAN ACLs (VLAN maps) for IPv6 traffic.

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

The active switch supports IPv6 ACLs in hardware and distributes the IPv6 ACLs to the stack members. If a standby switch takes over as the active switch, it distributes the ACL configuration to all stack members. The member switches sync up the configuration distributed by the new active switch and flush out entries that are not required.

When an ACL is modified, attached to, or detached from an interface, the active switch distributes the change to all stack members.

ACL Precedence

When Port ACLs, and router ACLs are configured on the same switch, the filtering precedence, from greatest to least for ingress traffic is port ACL, and then router ACL. For egress traffic, the filtering precedence is router ACL, and then port ACL.

The following examples describe simple use cases:

- 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.

VLAN Maps

VLAN ACLs or VLAN maps are used to control network traffic within a VLAN. You can apply VLAN maps to all packets that are bridged within a VLAN in the switch or switch stack. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VACLs are not defined by direction (ingress or egress).

All non-IP protocols are access-controlled through MAC addresses and Ethertype using MAC VLAN maps. (IP traffic is not access controlled by MAC VLAN maps.) You can enforce VLAN maps only on packets going through the switch; you cannot enforce VLAN maps on traffic between hosts on a hub or on another switch connected to this switch.

With VLAN maps, forwarding of packets is permitted or denied, based on the action specified in the map.

*Figure 20: Using VLAN Maps to Control Traffic*

This shows how a VLAN map is applied to prevent a specific type of traffic from Host A in VLAN 10 from being forwarded. You can apply only one VLAN map to a VLAN.
Interactions with Other Features and Switches

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

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

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

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

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

• If the hardware memory is full, packets are dropped on the interface and an unload error message is logged.

Restrictions for IPv6 ACLs

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

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

• The switch does not support matching on these keywords: routing header, and undetermined-transport.

• The switch does not support reflexive ACLs (the reflect keyword).

• This release supports port ACLs, router ACLs and VLAN ACLs (VLAN maps) for IPv6.

• The switch does not apply MAC-based ACLs on IPv6 frames.

• When configuring an ACL, there is no restriction on keywords entered in the ACL, regardless of whether or not they are supported on the platform. When you apply the ACL to an interface that requires hardware forwarding (physical ports or SVIs), the switch checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.

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

IPv6 ACLs on the switch have these characteristics:

• Fragmented frames (the fragments keyword as in IPv4) are supported

• The same statistics supported in IPv4 are supported for IPv6 ACLs.

• If the switch runs out of hardware space, the packets associated with the ACL are dropped on the interface.

• Logging is supported for router ACLs, but not for port ACLs.

• The switch supports IPv6 address-matching for a full range of prefix-lengths.
Default Configuration for IPv6 ACLs

The default IPv6 ACL configuration is as follows:

```
Switch# show access-lists preauth_ipv6_acl
IPv6 access list preauth_ipv6_acl (per-user)
permit udp any any eq domain sequence 10
permit tcp any any eq domain sequence 20
permit icmp any any nd-ns sequence 30
permit icmp any any nd-na sequence 40
permit icmp any any router-solicitation sequence 50
permit icmp any any router-advertisement sequence 60
permit icmp any any redirect sequence 70
permit udp any eq 547 any eq 546 sequence 80
permit udp any eq 546 any eq 547 sequence 90
deny ipv6 any any sequence 100
```

Configuring IPv6 ACLs

To filter IPv6 traffic, you perform these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>{ipv6 access-list list-name}</td>
<td>Defines an IPv6 ACL name, and enters IPv6 access list configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# ipv6 access-list example_acl_list</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>{deny</td>
<td>permit} protocol</td>
</tr>
<tr>
<td>{source-ipv6-prefix/prefix-length</td>
<td>any} host source-ipv6-address} [ operator [port-number]]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{destination-ipv6-prefix/prefix-length</td>
<td>any} host destination-ipv6-address} [operator [port-number][dscp value][fragments][log][log-input][sequence value][time-range name]}</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The <code>source-ipv6-prefix/prefix-length</code> or <code>destination-ipv6-prefix/ prefix-length</code> is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373).</td>
</tr>
<tr>
<td>• Enter any as an abbreviation for the IPv6 prefix <code>::/0</code>.</td>
</tr>
<tr>
<td>• For <strong>host</strong> <code>source-ipv6-address</code> or <code>destination-ipv6-address</code>, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td>• (Optional) For operator, specify an operand that compares the source or destination ports of the specified protocol. Operands are <code>lt</code> (less than), <code>gt</code> (greater than), <code>eq</code> (equal), <code>neq</code> (not equal), and <code>range</code>. If the operator follows the <code>source-ipv6-prefix/prefix-length</code> argument, it must match the source port. If the operator follows the <code>destination-ipv6-prefix/prefix-length</code> argument, it must match the destination port.</td>
</tr>
<tr>
<td>• (Optional) The <strong>port-number</strong> is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You can use UDP port names only when filtering UDP.</td>
</tr>
<tr>
<td>• (Optional) Enter <strong>dscp</strong> value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.</td>
</tr>
<tr>
<td>• (Optional) Enter <strong>fragments</strong> to check noninitial fragments. This keyword is visible only if the protocol is ipv6.</td>
</tr>
<tr>
<td>• (Optional) Enter <strong>log</strong> to cause a logging message to be sent to the console about</td>
</tr>
<tr>
<td>Command or Action</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
</tbody>
</table>
| {deny | permit} tcp <br>({source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [operator [port-number]] [ack] [dscp value] [established] [fin] [log] [log-input] [neq {port | protocol}] [psh] [range {port | protocol}] [rst] [sequence value] [syn] [time-range name] [urg]} | the packet that matches the entry. Enter **log-input** to include the input interface in the log entry. Logging is supported only for router ACLs.  
- (Optional) Enter **sequence value** to specify the sequence number for the access list statement. The acceptable range is from 1 to 4,294,967,295.  
- (Optional) Enter **time-range** name to specify the time range that applies to the deny or permit statement.  

**Step 5**<br>{deny | permit} udp <br>({source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [operator [port-number]] [dscp value] [log] [log-input] [neq {port | protocol}] [range {port | protocol}] | (Optional) Define a TCP access list and the access conditions.  
Enter tcp for Transmission Control Protocol. The parameters are the same as those described in Step 3a, with these additional optional parameters:  
- **ack**—Acknowledgment bit set.  
- **established**—An established connection. A match occurs if the TCP datagram has the ACK or RST bits set.  
- **fin**—Finished bit set; no more data from sender.  
- **neq {port | protocol}**—Matches only packets that are not on a given port number.  
- **psh**—Push function bit set.  
- **range {port | protocol}**—Matches only packets in the port number range.  
- **rst**—Reset bit set.  
- **syn**—Synchronize bit set.  
- **urg**—Urgent pointer bit set.  

**Step 6**<br>{deny | permit} udp <br>({source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [operator [port-number]] [dscp value] [log] [log-input] [neq {port | protocol}] [range {port | protocol}] | (Optional) Define a UDP access list and the access conditions.  
Enter udp for the User Datagram Protocol. The UDP parameters are the same as those described for TCP, except that the [operator [port]] port number or name must be a UDP
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol} [sequence value] [time-range name]]</td>
<td>port number or name, and the established parameter is not valid for UDP.</td>
</tr>
</tbody>
</table>

#### Step 7

{deny | permit} icmp
{source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]]
{destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [operator [port-number]] [icmp-type [icmp-code] | icmp-message] [dscp value] [log] [log-input]
[sequence value] [time-range name]

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

Enter `icmp` for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 1, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:

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

#### Step 8

**end**

Return to privileged EXEC mode.

#### Step 9

**show ipv6 access-list**

Verify the access list configuration.

#### Step 10

**show running-config**

Verifies your entries.

**Example:**

```
Device# show running-config
```

#### Step 11

**copy running-config startup-config**

(Optional) Saves your entries in the configuration file.

**Example:**

```
Device# copy running-config startup-config
```

### What to do next

Attach the IPv6 ACL to an Interface
### Attaching an IPv6 ACL to an Interface

You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces, or to inbound traffic on Layer 2 interfaces. You can also apply ACLs only to inbound management traffic on Layer 3 interfaces.

Follow these steps to control access to an interface:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><code>Device&gt;</code> <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>interface interface-id</code></td>
<td>Identify a Layer 2 interface (for port ACLs) or Layer 3 interface (for router ACLs) on which to apply an access list, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>no switchport</code></td>
<td>If applying a router ACL, this changes the interface from Layer 2 mode (the default) to Layer 3 mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>ipv6 address ipv6-address</code></td>
<td>Configure an IPv6 address on a Layer 3 interface (for router ACLs).</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>`ipv6 traffic-filter access-list-name {in</td>
<td>out}`</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# show running-config</code></td>
<td></td>
</tr>
</tbody>
</table>
To create a VLAN map and apply it to one or more VLANs, perform these steps:

**Before you begin**
Create the IPv6 ACL that you want to apply to the VLAN.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>vlan access-map name [number]</td>
<td>Creates a VLAN map, and give it a name and (optionally) a number. The number is the sequence number of the entry within the map.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete.</td>
</tr>
<tr>
<td></td>
<td>Device(config)# vlan access-map map_1 20</td>
<td>VLAN maps do not use the specific permit or deny keywords. To deny a packet by using VLAN maps, create an ACL that would match the packet, and set the action to drop. A permit in the ACL counts as a match. A deny in the ACL means no match.</td>
</tr>
</tbody>
</table>
## Applying a VLAN Map to a VLAN

Beginning in privileged EXEC mode, follow the procedure given below to apply a VLAN map to one or more VLANs:

### Step 4

**match {ip | ipv6 | mac} address {name | number} [name | number]**

**Example:**

```
Device(config-access-map)# match ipv6 address ip_net
```

**Purpose:**

Entering this command changes to access-map configuration mode.

**Step 5**

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:

- **action { forward}**
  
  **Example:**
  ```
  Device(config-access-map)# action forward
  ```

- **action { drop}**
  
  **Example:**
  ```
  Device(config-access-map)# action drop
  ```

**Purpose:**

Sets the action for the map entry.

**Step 6**

**vlan filter mapname vlan-list list**

**Example:**

```
Device(config)# vlan filter map 1 vlan-list 20-22
```

**Purpose:**

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.

---

### Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entering this command changes to access-map configuration mode.</td>
</tr>
<tr>
<td>Match the packet against one or more access lists. Note that packets are only matched against access lists of the correct protocol type. IP packets are matched against IP access lists. Non-IP packets are only matched against named MAC access lists.</td>
</tr>
<tr>
<td>Sets the action for the map entry.</td>
</tr>
<tr>
<td>Applies the VLAN map to one or more VLAN IDs.</td>
</tr>
</tbody>
</table>

### Example:

```
Device(config-access-map)# match ipv6 address ip_net
Device(config-access-map)# action forward
Device(config)# vlan filter map 1 vlan-list 20-22
```
**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vlan filter mapname vlan-list list</td>
<td>Applies the VLAN map to one or more VLAN IDs.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# vlan filter map 1 vlan-list 20-22</td>
<td>The list can be a single VLAN ID (22), a consecutive list (10-22), or a string of VLAN IDs (12, 22, 30). Spaces around the comma and hyphen are optional.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Displays the access list configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Monitoring IPv6 ACLs

You can display information about all configured access lists, all IPv6 access lists, or a specific access list by using one or more of the privileged EXEC commands shown in the table below:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show access-lists</td>
<td>Displays all access lists configured on the switch.</td>
</tr>
<tr>
<td>show ipv6 access-list [access-list-name]</td>
<td>Displays all configured IPv6 access lists or the access list specified by name.</td>
</tr>
<tr>
<td>show vlan access-map [map-name]</td>
<td>Displays VLAN access map configuration.</td>
</tr>
</tbody>
</table>
Purpose

Command

show vlan filter [access-map access-map| vlan vlan-id]

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vlan filter [access-map access-map</td>
<td>vlan vlan-id]</td>
</tr>
</tbody>
</table>

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

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

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

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

This is an example of the output from the show vlan access-map privileged EXEC command. The output shows VLAN access map information.

Switch# show vlan access-map
Vlan access-map "m1" 10
  Match clauses:
    ipv6 address: ip2
  Action: drop

Feature Information for IPv6 ACLs

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 47: Feature Information for IPv6 ACLs

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 ACLs</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>You can filter IPv6 traffic by creating IPv6 ACLs and applying them to interfaces similar to how you create and apply IPv4 named ACLs. You can also create and apply input router ACLs to filter Layer 3 management traffic when the switch is running IP base and LAN base feature sets.</td>
</tr>
</tbody>
</table>
CHAPTER 17

Configuring DHCP

- Information About DHCP, on page 309
- How to Configure DHCP Features, on page 315
- Configuring DHCP Server Port-Based Address Allocation, on page 321
- Feature Information for DHCP, on page 325

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.
For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces.

An untrusted DHCP message is a message that is received through an untrusted interface. By default, the switch considers all interfaces untrusted. So, the switch must be configured to trust some interfaces to use DHCP Snooping. When you use DHCP snooping in a service-provider environment, an untrusted message is sent from a device that is not in the service-provider network, such as a customer’s switch. Messages from unknown devices are untrusted because they can be sources of traffic attacks.

The DHCP snooping binding database has the MAC address, the IP address, the lease time, the binding type, the VLAN number, and the interface information that corresponds to the local untrusted interfaces of a switch. It does not have information regarding hosts interconnected with a trusted interface.

In a service-provider network, an example of an interface you might configure as trusted is one connected to a port on a device in the same network. An example of an untrusted interface is one that is connected to an untrusted interface in the network or to an interface on a device that is not in the network.

When a switch receives a packet on an untrusted interface and the interface belongs to a VLAN in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If the addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The switch drops a DHCP packet when one of these situations occurs:

- A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from outside the network or firewall.
- A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match.
- The switch receives a DHCPRELEASE or DHCPDECLINE broadcast message that has a MAC address in the DHCP snooping binding database, but the interface information in the binding database does not match the interface on which the message was received.
- A DHCP relay agent forwards a DHCP packet that includes a relay-agent IP address that is not 0.0.0.0, or the relay agent forwards a packet that includes option-82 information to an untrusted port.

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.
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.

The DHCP option-82 feature is supported only when DHCP snooping is globally enabled on the VLANs to which subscriber devices using option-82 are assigned.

The following illustration shows a metropolitan Ethernet network in which a centralized DHCP server assigns IP addresses to subscribers connected to the switch at the access layer. Because the DHCP clients and their associated DHCP server do not reside on the same IP network or subnet, a DHCP relay agent (the Catalyst switch) is configured with a helper address to enable broadcast forwarding and to transfer DHCP messages between the clients and the server.

When you enable the DHCP snooping information option 82 on the switch, the following sequence of events occurs:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the option-82 information in the packet. By default, the remote-ID suboption is the switch MAC address, and the circuit-ID suboption is the port identifier, `vlan-mod-port`, from which the packet is received. You can configure the remote ID and circuit ID.
- If the IP address of the relay agent is configured, the switch adds this IP address in the DHCP packet.
- The switch forwards the DHCP request that includes the option-82 field to the DHCP server.
- The DHCP server receives the packet. If the server is option-82-capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.
- The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. The switch verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.
In the default suboption configuration, when the described sequence of events occurs, the values in these fields do not change (see the illustration, *Suboption Packet Formats*):

- Circuit-ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Circuit-ID type
  - Length of the circuit-ID type

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

In the port field of the circuit ID suboption, the port numbers start at 3. For example, on a switch with 24 10/100/1000 ports and four small form-factor pluggable (SFP) module slots, port 3 is the Gigabit Ethernet 1/0/1 port, port 4 is the Gigabit Ethernet 1/0/2 port, and so forth. Port 27 is the SFP module slot Gigabit Ethernet1/0/25, and so forth.

The illustration, *Suboption Packet Formats*, shows the packet formats for the remote-ID suboption and the circuit-ID suboption when the default suboption configuration is used. For the circuit-ID suboption, the module number corresponds to the switch number in the stack. The switch uses the packet formats when you globally enable DHCP snooping and enter the `ip dhcp snooping information option global configuration command`.

---

**Figure 22: Suboption Packet Formats**

**Circuit ID Suboption Frame Format**

<table>
<thead>
<tr>
<th>Suboption type</th>
<th>Circuit-ID type</th>
<th>Length</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 byte</td>
<td>1 byte</td>
<td>1 byte</td>
<td>1 byte</td>
</tr>
</tbody>
</table>

**Remote ID Suboption Frame Format**

<table>
<thead>
<tr>
<th>Suboption type</th>
<th>Remote-ID type</th>
<th>Length</th>
<th>Length</th>
<th>MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 byte</td>
<td>1 byte</td>
<td>1 byte</td>
<td>1 byte</td>
<td>6 bytes</td>
</tr>
</tbody>
</table>

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 23: User-Configured Suboption Packet Formats

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

```
<table>
<thead>
<tr>
<th>Suboption type</th>
<th>Circuit ID type</th>
<th>Length</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N+2</td>
<td>1</td>
<td>N</td>
</tr>
</tbody>
</table>
```

1 byte 1 byte 1 byte 1 byte N bytes (N = 3-63)

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

```
<table>
<thead>
<tr>
<th>Suboption type</th>
<th>Remote ID type</th>
<th>Length</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>N+2</td>
<td>1</td>
<td>N</td>
</tr>
</tbody>
</table>
```

1 byte 1 byte 1 byte 1 byte N bytes (N = 1-63)

### 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-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>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP server</td>
<td>Enabled in Cisco IOS software, requires configuration</td>
</tr>
<tr>
<td>DHCP relay agent</td>
<td>Enabled</td>
</tr>
<tr>
<td>DHCP packet forwarding address</td>
<td>None configured</td>
</tr>
<tr>
<td>Checking the relay agent information</td>
<td>Enabled (invalid messages are dropped)</td>
</tr>
<tr>
<td>DHCP relay agent forwarding policy</td>
<td>Replace the existing relay agent information</td>
</tr>
<tr>
<td>DHCP snooping enabled globally</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping information option</td>
<td>Enabled</td>
</tr>
<tr>
<td>DHCP snooping option to accept packets on untrusted input interfaces</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping limit rate</td>
<td>None configured</td>
</tr>
<tr>
<td>Feature</td>
<td>Default Setting</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DHCP snooping trust</td>
<td>Untrusted</td>
</tr>
<tr>
<td>DHCP snooping VLAN</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping MAC address verification</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cisco IOS DHCP server binding database</td>
<td>Enabled in Cisco IOS software, requires configuration. The switch gets network addresses and configuration parameters only from a device configured as a DHCP server.</td>
</tr>
<tr>
<td>DHCP snooping binding database agent</td>
<td>Enabled in Cisco IOS software, requires configuration. This feature is operational only when a destination is configured.</td>
</tr>
</tbody>
</table>

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

- If a switch port is connected to a DHCP server, configure a port as trusted by entering the `ip dhcp snooping trust interface` configuration command.
- If a switch port is connected to a DHCP client, configure a port as untrusted by entering the `no ip dhcp snooping trust` interface configuration command.
- You can display DHCP snooping statistics by entering the `show ip dhcp snooping statistics` user EXEC command, and you can clear the snooping statistics counters by entering the `clear ip dhcp snooping statistics` privileged EXEC command.

Configuring the DHCP Server

The switch can act as a DHCP server.

For procedures to configure the switch as a DHCP server, see the “Configuring DHCP” section of the “IP addressing and Services” section of the *Cisco IOS IP Configuration Guide, Release 12.4.*

DHCP Server and Switch Stacks

The DHCP binding database is managed on the stack master. When a new stack master is assigned, the new master downloads the saved binding database from the TFTP server. When a switchover happens, the new active stack master will use its database file that has been synced from the old active stack master using the SSO function. The IP addresses associated with the lost bindings are released. You should configure an automatic backup by using the `ip dhcp database url [timeout seconds | write-delay seconds]` global configuration command.
Configuring the DHCP Relay Agent

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

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable&lt;br&gt;Example: Device&gt; enable</td>
<td>Enables privileged EXEC mode.&lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal&lt;br&gt;Example: Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>service dhcp&lt;br&gt;Example: Device(config)# service dhcp</td>
<td>Enables the DHCP server and relay agent on your switch. By default, this feature is enabled.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end&lt;br&gt;Example: Device(config)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config&lt;br&gt;Example: Device# show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config&lt;br&gt;Example: Device# copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**What to do next**

- Checking (validating) the relay agent information
- Configuring the relay agent forwarding policy
Specifying the Packet Forwarding Address

If the DHCP server and the DHCP clients are on different networks or subnets, you must configure the switch with the `ip helper-address address` interface configuration command. The general rule is to configure the command on the Layer 3 interface closest to the client. The address used in the `ip helper-address` command can be a specific DHCP server IP address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables any DHCP server to respond to requests.

Beginning in privileged EXEC mode, follow these steps to specify the packet forwarding address:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates a switch virtual interface by entering a VLAN ID, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>interface vlan vlan-id</td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface vlan 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the interface with an IP address and an IP subnet.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>ip address ip-address subnet-mask</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ip address 192.108.1.27 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Specifies the DHCP packet forwarding address.</td>
</tr>
<tr>
<td>Example:</td>
<td>The helper address can be a specific DHCP server address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables other servers to respond to DHCP requests.</td>
</tr>
<tr>
<td>ip helper-address address</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ip helper-address 172.16.1.2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Device(config-if)# end</td>
<td>Configures multiple physical ports that are connected to the DHCP clients, and enter interface range configuration mode. Or Configures a single physical port that is connected to the DHCP client, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>

**Step 7**

Use one of the following:

- `interface range port-range`
- `interface interface-id`

**Example:**

Device(config)# interface gigabitethernet1/0/2

**Step 8**

`switchport mode access`

**Example:**

Device(config-if)# switchport mode access

**Step 9**

`switchport access vlan vlan-id`

**Example:**

Device(config-if)# switchport access vlan 1

**Step 10**

`end`

**Example:**

Device(config-if)# end

**Step 11**

`show running-config`

**Example:**

Device# show running-config

**Step 12**

`copy running-config startup-config`

**Example:**

Device# copy running-config startup-config

---

**Prerequisites for Configuring DHCP Snooping and Option 82**

The prerequisites for DHCP Snooping and Option 82 are as follows:

- You must globally enable DHCP snooping on the switch.
- Before globally enabling DHCP snooping on the switch, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
• If you want the switch to respond to DHCP requests, it must be configured as a DHCP server.

• Before configuring the DHCP snooping information option on your switch, be sure to configure the device that is acting as the DHCP server. You must specify the IP addresses that the DHCP server can assign or exclude, or you must configure DHCP options for these devices.

• For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces. In a service-provider network, a trusted interface is connected to a port on a device in the same network.

• You must configure the switch to use the Cisco IOS DHCP server binding database to use it for DHCP snooping.

• To use the DHCP snooping option of accepting packets on untrusted inputs, the switch must be an aggregation switch that receives packets with option-82 information from an edge switch.

• The following prerequisites apply to DHCP snooping binding database configuration:
  • You must configure a destination on the DHCP snooping binding database to use the switch for DHCP snooping.
  • Because both NVRAM and the flash memory have limited storage capacity, we recommend that you store the binding file on a TFTP server.
  • For network-based URLs (such as TFTP and FTP), you must create an empty file at the configured URL before the switch can write bindings to the binding file at that URL. See the documentation for your TFTP server to determine whether you must first create an empty file on the server; some TFTP servers cannot be configured this way.
  • To ensure that the lease time in the database is accurate, we recommend that you enable and configure Network Time Protocol (NTP).
  • If NTP is configured, the switch writes binding changes to the binding file only when the switch system clock is synchronized with NTP.

• Before configuring the DHCP relay agent on your switch, make sure to configure the device that is acting as the DHCP server. You must specify the IP addresses that the DHCP server can assign or exclude, configure DHCP options for devices, or set up the DHCP database agent.

• If you want the switch to relay DHCP packets, the IP address of the DHCP server must be configured on the switch virtual interface (SVI) of the DHCP client.

• If a switch port is connected to a DHCP server, configure a port as trusted by entering the `ip dhcp snooping trust interface` configuration command.

• If a switch port is connected to a DHCP client, configure a port as untrusted by entering the `no ip dhcp snooping trust` interface configuration command.

### Enabling 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 49: Commands for Displaying DHCP Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip dhcp snooping</code></td>
<td>Displays the DHCP snooping configuration for a switch</td>
</tr>
<tr>
<td><code>show ip dhcp snooping binding</code></td>
<td>Displays only the dynamically configured bindings in the DHCP snooping binding database, also referred to as a binding table.</td>
</tr>
<tr>
<td><code>show ip dhcp snooping database</code></td>
<td>Displays the DHCP snooping binding database status and statistics.</td>
</tr>
<tr>
<td><code>show ip dhcp snooping statistics</code></td>
<td>Displays the DHCP snooping statistics in summary or detail form.</td>
</tr>
<tr>
<td><code>show ip source binding</code></td>
<td>Display the dynamically and statically configured bindings.</td>
</tr>
</tbody>
</table>

**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.
- To restrict assignments from the DHCP pool to preconfigured reservations (unreserved addresses are not offered to the client and other clients are not served by the pool), you can enter the reserved-only DHCP pool configuration command.

Enabling the DHCP Snooping Binding Database Agent

Beginning in privileged EXEC mode, follow these steps to enable and configure the DHCP snooping binding database agent on the switch:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ip dhcp snooping database flash[</td>
<td>Specifies the URL for the database agent or the binding file by using one of these forms:</td>
</tr>
<tr>
<td></td>
<td>number]:/filename</td>
<td>• flash[number]:/filename</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional) Use the number parameter to specify the stack member number of the stack master. The range for number is 1 to 9.</td>
</tr>
<tr>
<td></td>
<td>ftp://user:password@host/filename</td>
<td></td>
</tr>
<tr>
<td></td>
<td>http://[username:password]@[hostname</td>
<td></td>
</tr>
<tr>
<td></td>
<td>host-ip]/[directory] image-name.tar</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rcp://user@host/filename</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tftp://host/filename</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ftp://user:password@host/filename</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• http://[username:password]@[hostname</td>
</tr>
<tr>
<td></td>
<td></td>
<td>host-ip]/[directory] image-name.tar</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• rcp://user@host/filename</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>ip dhcp snooping database timeout seconds</code></td>
<td>Specifies (in seconds) how long to wait for the database transfer process to finish before stopping the process. The default is 300 seconds. The range is 0 to 86400. Use 0 to define an infinite duration, which means to continue trying the transfer indefinitely.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>ip dhcp snooping database timeout 300</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>ip dhcp snooping database write-delay seconds</code></td>
<td>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).</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>ip dhcp snooping database write-delay 15</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> <code>ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds</code></td>
<td>(Optional) Adds binding entries to the DHCP snooping binding database. The <code>vlan-id</code> range is from 1 to 4904. The <code>seconds</code> range is from 1 to 4294967295. Enter this command for each entry that you add. Use this command when you are testing or debugging the switch.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# <code>ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> <code>show ip dhcp snooping database [detail]</code></td>
<td>Displays the status and statistics of the DHCP snooping binding database agent.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# <code>show ip dhcp snooping database detail</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> <code>show running-config</code></td>
<td>Verifies your entries.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# <code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> <code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# <code>copy running-config</code></td>
<td></td>
</tr>
</tbody>
</table>
Enabling DHCP Server Port-Based Address Allocation

Follow these steps to globally enable port-based address allocation and to automatically generate a subscriber identifier on an interface.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>startup-config</strong></td>
<td>Enabling DHCP server port-based address allocation.</td>
</tr>
</tbody>
</table>

**Step 1**
- **enable**
  - Example:
    ```
    Device> enable
    ```

**Step 2**
- **configure terminal**
  - Example:
    ```
    Device# configure terminal
    ```

**Step 3**
- **ip dhcp use subscriber-id client-id**
  - Example:
    ```
    Device(config)# ip dhcp use subscriber-id client-id
    ```

**Step 4**
- **ip dhcp subscriber-id interface-name**
  - Example:
    ```
    Device(config)# ip dhcp subscriber-id interface-name
    ```

**Step 5**
- **interface interface-id**
  - Example:
    ```
    Device(config)# interface gigabitethernet1/0/1
    ```

**Step 6**
- **ip dhcp server use subscriber-id client-id**
  - Example:
    ```
    Device(config-if)# ip dhcp server use subscriber-id client-id
    ```
### Purpose

#### Command or Action

**Step 7**

**end**  
*Example:*

```
Device(config)# end
```

**Step 8**

**show running-config**  
*Example:*

```
Device# show running-config
```

**Step 9**

**copy running-config startup-config**  
*Example:*

```
Device# copy running-config startup-config
```

#### Purpose

- Returns to privileged EXEC mode.
- Verifies your entries.
- (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 50: Commands for Displaying DHCP Port-Based Address Allocation Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interface interface id</code></td>
<td>Displays the status and configuration of a specific interface.</td>
</tr>
<tr>
<td><code>show ip dhcp pool</code></td>
<td>Displays the DHCP address pools.</td>
</tr>
<tr>
<td><code>show ip dhcp binding</code></td>
<td>Displays address bindings on the Cisco IOS DHCP server.</td>
</tr>
</tbody>
</table>

### Feature Information for DHCP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.
### Table 51: Feature Information for DHCP

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>DHCP provides configuration parameters to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP Server to a host and a mechanism for allocating network addresses to hosts. DHCP is built on a client/server model, where designated DHCP Server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.</td>
</tr>
<tr>
<td>DHCP Client Option 12</td>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>The DHCP Client Option 12 feature specifies the hostname of the client. While acquiring an IP address for an interface from the Dynamic Host Configuration Protocol (DHCP) server, if the client device receives the DHCP Hostname option inside the response, the hostname from that option is set. DHCP is used by DHCP clients to obtain configuration information for operation in an IP network.</td>
</tr>
</tbody>
</table>
CHAPTER 18

DHCPv6 Options Support

This module describes the CAPWAP Access Controller DHCPv6 Option (DHCPv6 Option 52), DHCPv6 Client Link-Layer Address Option, and DNS Search List features.

CAPWAP is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points.

RFC 6939 defines a mechanism to allow first-hop DHCPv6 relay agents (relay agents that are connected to the same link as the client) to provide the client's link-layer address in DHCPv6 messages being sent towards the server. This feature is enabled by default, when DHCP relay is configured.

DNS Search List (DNSSL) is a list of Domain Name System (DNS) suffix domain names used by IPv6 hosts when they perform DNS query searches for short, unqualified domain names.

• Information About DHCPv6 Options Support, on page 327
• How to Configure DHCPv6 Options Support, on page 329
• Configuration Examples for DHCPv6 Options Support, on page 331
• Verifying DHCPv6 Options Support, on page 331
• Feature Information for DHCPv6 Options Support, on page 333

Information About DHCPv6 Options Support

CAPWAP Access Controller DHCPv6 Option

The Control And Provisioning of Wireless Access Points (CAPWAP) protocol allows lightweight access points to use DHCPv6 to discover a wireless controller to which it can connect. CAPWAP is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points.

Wireless access points use the DHCPv6 option 52 (RFC 5417) to supply the IPv6 management interface addresses of the primary, secondary, and tertiary wireless controllers.

Both stateless and stateful DHCPv6 addressing modes are supported. In stateless mode, access points obtain IPv6 address using the Stateless Address AutoConfiguration (SLAAC), while additional network information (not obtained from router advertisements) is obtained from a DHCPv6 server. In stateful mode, access points obtain both IPv6 addressing and additional network information exclusively from the DHCPv6 server. In both modes, a DHCPv6 server is required to provide option 52 if Wireless Controller discovery using DHCPv6 is required.
DNS Search List Option

DNS Search List (DNSSL) is a list of Domain Name System (DNS) suffix domain names used by IPv6 hosts when they perform DNS query searches for short, unqualified domain names. The DNSSL option contains one or more domain names. All domain names share the same lifetime value, which is the maximum time in seconds over which this DNSSL may be used. If different lifetime values are required, multiple DNSSL options can be used. There can be a maximum of 5 DNSSLs.

If DNS information is available from multiple Router Advertisements (RAs) and/or from DHCP, the host must maintain an ordered list of this DNS information.

RFC 6106 specifies IPv6 Router Advertisement (RA) options to allow IPv6 routers to advertise a DNS Search List (DNSSL) to IPv6 hosts for an enhanced DNS configuration.

The DNS lifetime range should be between the maximum RA interval and twice the maximum RA interval, as displayed in the following example:

\[(\text{max ra interval}) \leq \text{dns lifetime} \leq (2\times\text{max ra interval})\]

The maximum RA interval can have a value between 4 and 1800 seconds (the default is 240 seconds). The following example shows an out-of-range lifetime:

```
Device(config-if)# ipv6 nd ra dns search list sss.com 3600
! Lifetime configured out of range for the interface that has the default maximum RA interval.!
```

DHCPv6 Client Link-Layer Address Option

Cisco IOS XE Fuji 16.8.1a supports DHCPv6 Client Link-Layer Address Option (RFC 6939). It defines an optional mechanism and the related DHCPv6 option to allow first-hop DHCPv6 relay agents (relay agents that are connected to the same link as the client) to provide the client's link-layer address in DHCPv6 messages that are sent towards the server.

The Client Link-Layer Address option is only exchanged between relay agents and servers. DHCPv6 clients are not aware of the use of the Client Link-Layer Address option. The DHCPv6 client must not send the Client Link-Layer Address option, and must ignore the Client Link-Layer Address option if received.

Each DHCPv6 client and server is identified by a DHCP unique identifier (DUID). The DUID is carried in the client identifier and server identifier options. The DUID is unique across all DHCP clients and servers, and it is stable for any specific client or server. DHCPv6 uses DUIDs based on link-layer addresses for both the client and server identifier. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device.

DHCPv6 Relay Agent

A DHCPv6 relay agent, which may reside on a client link, is used to relay messages between the client and the server. The DHCPv6 relay agent operation is transparent to the client. The DHCPv6 client locates a DHCPv6 server using a reserved, link-scoped multicast address. For direct communication between the DHCPv6 client and the DHCPv6 server, both of them must be attached to the same link. However, in some
situations where ease of management, economy, or scalability is a concern, it is desirable to allow a DHCPv6 client to send messages to a DHCPv6 server that is not connected to the same link. IPv6 enable is required for IPv6 DHCP relay, even if the IPv6 address is configured.

### How to Configure DHCPv6 Options Support

#### Configuring CAPWAP Access Points

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable  
Example:  
Device> enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Step 2** | configure terminal  
Example:  
Device# configure terminal | Enters global configuration mode. |
| **Step 3** | ipv6 dhcp pool poolname  
Example:  
Device(config)# ipv6 dhcp pool pool1 | Configures a DHCPv6 server configuration information pool and enters DHCPv6 pool configuration mode. |
| **Step 4** | capwap-ac address ipv6-address  
Example:  
Device(config-dhcpv6)# capwap-ac address 2001:DB8::1 | Configures CAPWAP access controller address. |
| **Step 5** | end  
Example:  
Device(config-dhcpv6)# end | Exits DHCPv6 pool configuration mode and returns to privileged EXEC mode. |

### Configuring DNS Search List Using IPv6 Router Advertisement Options

**Note**  
The domain name configuration should follow RFC 1035. If not, the configuration will be rejected. For example, the following domain name configuration will result in an error:  

```
Device(config-if)# ipv6 nd ra dns search list .example.example.com infinite-lifetime
```

Use the `no ipv6 nd ra dns search list name` command to delete a single DNS search list under an interface.  
Use the `no ipv6 nd ra dns search list` command to delete all DNS search lists under an interface.
## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | **enable** | Enables privileged EXEC mode.  
*Example:*  
Device> enable |
| Step 2 | **configure terminal** | Enters global configuration mode.  
*Example:*  
Device# configure terminal |
| Step 3 | **interface interface-type interface-number** | Configures an interface and enters interface configuration mode.  
*Example:*  
Device(config)# interface GigabitEthernet 0/2/0 |
| Step 4 | **ipv6 nd prefix ipv6-prefix/prefix-length** | Configures IPv6 prefixes that are included in IPv6 Neighbor Discovery (ND) router advertisements,  
*Example:*  
Device(config-if)# ipv6 nd prefix 2001:DB8::1/64 1111 222 |
| Step 5 | **ipv6 nd ra lifetime seconds** | Configures the device lifetime value in IPv6 router advertisements on an interface.  
*Example:*  
Device(config-if)# ipv6 nd ra lifetime 9000 |
| Step 6 | **ipv6 nd ra dns search list list-name [infinite-lifetime]** | Configures the DNS search list. You can specify the life time of the search list.  
*Example:*  
Device(config-if)# ipv6 nd ra dns search list example.example.com infinite-lifetime |
| Step 7 | **end** | Exits interface configuration mode and returns to privileged EXEC mode.  
*Example:*  
Device(config-if)# end |

### What to do next

Use the `show ipv6 nd idb interface` command to verify the DNS search list configuration based on IPv6 RA options:

```
Device# show ipv6 nd idb interface gigabitEthernet 0/2/0/0 detail location 0/2/CPU0
```

```
Mon Jul 4 14:28:53.422 IST
ifname: Gi0/2/0/0, ifh: 0x01000300, iftype: 15, VI-type: 0, Pseudo IDB: FALSE
vrf-id: 0x60000000, table-id: 0xe0800000
Mac Addr: 02d1.1e2b.0baf, size: 6, VLan tag set: FALSE
```
Configuration Examples for DHCPv6 Options Support

Example: Configuring CAPWAP Access Points

The following example shows how to configure a CAPWAP access point:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp pool pool1
Device(config-dhcpv6)# capwap-ac address 2001:DB8::1
Device(config-dhcpv6)# end
Device#
```

Verifying DHCPv6 Options Support

Verifying Option 52 Support

The following sample output from the `show ipv6 dhcp pool` command displays the DHCPv6 configuration information:

```
Device# show ipv6 dhcp pool

DHCPv6 pool: svr-p1
Static bindings:
   Binding for client 000300010002FCA5C01C
      IA PD: IA ID 00040002,
      Prefix: 2001:db8::3/72
      preferred lifetime 604800, valid lifetime 2592000
   IA PD: IA ID not specified; being used by 00040001
      Prefix: 2001:db8::1/72
      preferred lifetime 240, valid lifetime 54321
   Prefix: 2001:db8::2/72
      preferred lifetime 300, valid lifetime 54333
      Prefix: 2001:db8::3/72
```
preferred lifetime 280, valid lifetime 51111
Prefix from pool: local-p1, Valid lifetime 12345, Preferred lifetime 180
DNS server: 1001::1
DNS server: 1001::2
CAPWAP-AC Controller address: 2001:DB8::1
Domain name: example1.com
Domain name: example2.com
Domain name: example3.com
Active clients: 2

The following example shows how to enable debugging for DHCPv6:

Device# debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)

Troubleshooting DNS Search Lists

Recursive DNS servers and DNS search lists are sent as part of RA messages. Run the IPv6 ND traces to
dump any particular issue related to a DNS servers and DNS search lists:

Device# show ipv6 nd trace location 0/2/CPU0

Jun 30 20:07:03.508 nd/fevent 0/2/CPU0 t26702 Sending RA to ff02::1 on GigabitEthernet0/2/0/0
(0x1000300)
Jun 30 20:07:03.508 nd/fevent 0/2/CPU0 t26702 hoplimit 64 lifetime 9000 reachable 0 retrans
0
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 1::/64 Onlink Auto
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 valid 2592000 pref 604800
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 2002:4898:e8:1011::/64 Onlink Auto
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 valid 1111 pref 222
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 valid 1111 pref 222
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 valid 1111 pref 222
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 valid 1111 pref 222
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 valid 1111 pref 222
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra specific route address 3:: lifetime 1112
preference Low
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns server address 5::6 lifetime 240 first
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns server address 5::5 lifetime 240 part
of same ra dns server option
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns server address 4::4 lifetime 4294967295
first
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns search list name example.example.com
lifetime 240 first
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns search list name example1.example1.com
lifetime 240 part of
same ra dns search list option
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns search list name example2.example2.com
lifetime 4294967295 first
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 nd_send_ra: sending RA paksize=320, plen=280
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 nd_pak_send: size=320, ifh
GigabitEthernet0/2/0/0 (0x1000300),
priority=2 to ipv6-10
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 nd_pak_send: sending pak=0x60c07d8b with NO
FVS set, size=320,
ifh GigabitEthernet0/2/0/0 (0x1000300) to ipv6-10
Feature Information for DHCPv6 Options Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPWAP Access Controller DHCPv6 Option-52</td>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>The CAPWAP protocol allows lightweight access points to use DHCPv6 to discover a Wireless Controller to which it can connect. CAPWAP is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points.</td>
</tr>
<tr>
<td>DHCPv6 Client Link-Layer Address Option</td>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>The DHCPv6 Client Link-Layer Address Option (RFC 6939) defines an optional mechanism and the related DHCPv6 option to allow first-hop DHCPv6 relay agents (relay agents that are connected to the same link as the client) to provide the client's link-layer address in the DHCPv6 messages being sent towards the server.</td>
</tr>
<tr>
<td>DNS Search List</td>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>DNS Search List (DNSSL) is a list of Domain Name System (DNS) suffix domain names used by IPv6 hosts when they perform DNS query searches for short, unqualified domain names. The DNSSL option contains one or more domain names.</td>
</tr>
</tbody>
</table>
Feature Information for DHCPv6 Options Support
CHAPTER 19

Configuring IP Source Guard

• Information About IP Source Guard, on page 335
• How to Configure IP Source Guard, on page 337
• Monitoring IP Source Guard, on page 339
• Additional References, on page 340
• Feature Information for IP Source Guard, on page 340

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 device-tracking database` 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` command in global configuration mode on a routed interface, this error message appears:

  Static IP source binding can only be configured on switch port.

- When IP source guard with source IP filtering is enabled on an interface, DHCP snooping must be enabled on the access VLAN for that interface.

- If you are enabling IP source guard on a trunk interface with multiple VLANs and DHCP snooping is enabled on all the VLANs, the source IP address filter is applied on all the VLANs.

**Note**

If IP source guard is enabled and you enable or disable DHCP snooping on a VLAN on the trunk interface, the switch might not properly filter traffic.

- You can enable this feature when 802.1x port-based authentication is enabled.
# How to Configure IP Source Guard

## Enabling IP Source Guard

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable<br>**Example:**<br>Device> enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Step 2** | configure terminal<br>**Example:**<br>Device# configure terminal | Enters global configuration mode. |
| **Step 3** | interface interface-id<br>**Example:**<br>Device(config)# interface gigabitethernet 1/0/1 | Specifies the interface to be configured, and enters interface configuration mode. |
| **Step 4** | exit<br>**Example:**<br>Device(config-if)# exit | Returns to global configuration mode. |
| **Step 5** | ip source binding mac-address vlan vlan-id ip-address interface interface-id<br>**Example:**<br>Device(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1 | Adds a static IP source binding.  
Enter this command for each static binding. |
| **Step 6** | end<br>**Example:**<br>Device(config)# end | Returns to privileged EXEC mode. |
### Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port

You must configure the `ip device tracking maximum limit-number` interface configuration command globally for IPSG for static hosts to work. If you only configure this command on a port without enabling IP device tracking globally or by setting an IP device tracking maximum on that interface, IPSG with static hosts rejects all the IP traffic from that interface.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
  * Enter your password if prompted. |
| Step 2 | `configure terminal` | Enters global configuration mode. |
| Step 3 | `ip device tracking` | Turns on the IP host table, and globally enables IP device tracking. |
| Step 4 | `interface interface-id` | Enters interface configuration mode. |

---

#### Configuring IP Source Guard

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**Example:**

**Step 7**

```
Device# show running-config
```

**Step 8**

```
Device# copy running-config startup-config
```
### Configuring IP Source Guard

#### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td><code>switchport mode access</code></td>
<td>Configures a port as access.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-if)# switchport mode access</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>switchport access vlan vlan-id</code></td>
<td>Configures the VLAN for this port.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-if)# switchport access vlan 10</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>ip device tracking maximum number</code></td>
<td>Establishes a maximum limit for the number of static IPs that the IP device tracking table allows on the port. The range is 1 to 10. The maximum number is 10.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-if)# ip device tracking maximum 8</code></td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>You must configure the <code>ip device tracking maximum limit-number</code> interface configuration command.</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

### Monitoring IP Source Guard

#### Table 53: Privileged EXEC show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip verify source [ interface interface-id ]</code></td>
<td>Displays the IP source guard configuration on the switch or on a specific interface.</td>
</tr>
<tr>
<td>`show ip device tracking { all</td>
<td>interface interface-id</td>
</tr>
</tbody>
</table>

#### Table 54: Interface Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip verify source tracking</code></td>
<td>Verifies the data source.</td>
</tr>
</tbody>
</table>

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

Error Message Decoder

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

MIBs

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

Technical Assistance

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

Feature Information for IP Source Guard

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
### Table 55: Feature Information for IP Source Guard

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Source Guard</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>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.</td>
</tr>
</tbody>
</table>
Restrictions for Dynamic ARP Inspection

This section lists the restrictions and guidelines for configuring Dynamic ARP Inspection on the switch.

- Dynamic ARP inspection is an ingress security feature; it does not perform any egress checking.

- Dynamic ARP inspection is not effective for hosts connected to switches that do not support dynamic ARP inspection or that do not have this feature enabled. Because man-in-the-middle attacks are limited to a single Layer 2 broadcast domain, separate the domain with dynamic ARP inspection checks from the one with no checking. This action secures the ARP caches of hosts in the domain enabled for dynamic ARP inspection.

- Dynamic ARP inspection depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses.

  When DHCP snooping is disabled or in non-DHCP environments, use ARP ACLs to permit or to deny packets.

- Dynamic ARP inspection is supported on access ports, trunk ports, and EtherChannel ports.
Do not enable Dynamic ARP inspection on RSPAN VLANs. If Dynamic ARP inspection is enabled on RSPAN VLANs, Dynamic ARP inspection packets might not reach the RSPAN destination port.

- A physical port can join an EtherChannel port channel only when the trust state of the physical port and the channel port match. Otherwise, the physical port remains suspended in the port channel. A port channel inherits its trust state from the first physical port that joins the channel. Consequently, the trust state of the first physical port need not match the trust state of the channel.

  Conversely, when you change the trust state on the port channel, the switch configures a new trust state on all the physical ports that comprise the channel.

- The rate limit is calculated separately on each switch in a switch stack. For a cross-stack EtherChannel, this means that the actual rate limit might be higher than the configured value. For example, if you set the rate limit to 30 pps on an EtherChannel that has one port on switch 1 and one port on switch 2, each port can receive packets at 29 pps without causing the EtherChannel to become error-disabled.

- The operating rate for the port channel is cumulative across all the physical ports within the channel. For example, if you configure the port channel with an ARP rate-limit of 400 pps, all the interfaces combined on the channel receive an aggregate 400 pps. The rate of incoming ARP packets on EtherChannel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for EtherChannel ports only after examining the rate of incoming ARP packets on the channel-port members.

  The rate of incoming packets on a physical port is checked against the port-channel configuration rather than the physical-ports configuration. The rate-limit configuration on a port channel is independent of the configuration on its physical ports.

  If the EtherChannel receives more ARP packets than the configured rate, the channel (including all physical ports) is placed in the error-disabled state.

- Make sure to limit the rate of ARP packets on incoming trunk ports. Configure trunk ports with higher rates to reflect their aggregation and to handle packets across multiple dynamic ARP inspection-enabled VLANs. You also can use the `ip arp inspection limit none` interface configuration command to make the rate unlimited. A high rate-limit on one VLAN can cause a denial-of-service attack to other VLANs when the software places the port in the error-disabled state.

- When you enable dynamic ARP inspection on the switch, policers that were configured to police ARP traffic are no longer effective. The result is that all ARP traffic is sent to the CPU.

**Understanding Dynamic ARP Inspection**

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, Host B wants to send information to Host A but does not have the MAC address of Host A in its ARP cache. Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All hosts within the broadcast domain receive the ARP request, and Host A responds with its MAC address. However, because ARP allows a gratuitous reply from a host even if an ARP request was not received, an ARP spoofing attack and the poisoning of ARP caches can occur. After the attack, all traffic from the device under attack flows through the attacker’s computer and then to the router, switch, or host.
A malicious user can attack hosts, switches, and routers connected to your Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. Figure 26-1 shows an example of ARP cache poisoning.

**Figure 24: 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 25: 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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic ARP inspection</td>
<td>Disabled on all VLANs.</td>
</tr>
<tr>
<td>Interface trust state</td>
<td>All interfaces are untrusted.</td>
</tr>
<tr>
<td>Rate limit of incoming ARP packets</td>
<td>The rate is 15 pps on untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second. The rate is unlimited on all trusted interfaces. The burst interval is 1 second.</td>
</tr>
<tr>
<td>ARP ACLs for non-DHCP environments</td>
<td>No ARP ACLs are defined.</td>
</tr>
<tr>
<td>Validation checks</td>
<td>No checks are performed.</td>
</tr>
<tr>
<td>Log buffer</td>
<td>When dynamic ARP inspection is enabled, all denied or dropped ARP packets are logged.</td>
</tr>
<tr>
<td>Per-VLAN logging</td>
<td>All denied or dropped ARP packets are logged.</td>
</tr>
</tbody>
</table>

Relative Priority of ARP ACLs and DHCP Snooping Entries

Dynamic ARP inspection uses the DHCP snooping binding database for the list of valid IP-to-MAC address bindings.

ARP ACLs take precedence over entries in the DHCP snooping binding database. The switch uses ACLs only if you configure them by using the ip arp inspection filter vlan global configuration command. The switch first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the switch also denies the packet even if a valid binding exists in the database populated by DHCP snooping.

Configuring ARP ACLs for Non-DHCP Environments

This procedure shows how to configure dynamic ARP inspection when Switch B shown in Figure 2 does not support dynamic ARP inspection or DHCP snooping.

If you configure port 1 on Switch A as trusted, a security hole is created because both Switch A and Host 1 could be attacked by either Switch B or Host 2. To prevent this possibility, you must configure port 1 on Switch A as untrusted. To permit ARP packets from Host 2, you must set up an ARP ACL and apply it to VLAN 1. If the IP address of Host 2 is not static (it is impossible to apply the ACL configuration on Switch A) you must separate Switch A from Switch B at Layer 3 and use a router to route packets between them.
Follow these steps to configure an ARP ACL on Switch A. This procedure is required in non-DHCP environments.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>arp access-list acl-name</td>
<td>Defines an ARP ACL, and enters ARP access-list configuration mode. By default, no ARP access lists are defined.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>At the end of the ARP access list, there is an implicit deny ip any mac any command.</td>
</tr>
<tr>
<td>4</td>
<td>permit ip host sender-ip mac host sender-mac</td>
<td>Permits ARP packets from the specified host (Host 2).</td>
</tr>
<tr>
<td></td>
<td>• For sender-ip, enter the IP address of Host 2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For sender-mac, enter the MAC address of Host 2.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>6</td>
<td>ip arp inspection filter arp-acl-name vlan vlan-range [static]</td>
<td>Applies ARP ACL to the VLAN. By default, no defined ARP ACLs are applied to any VLAN.</td>
</tr>
<tr>
<td></td>
<td>• For arp-acl-name, specify the name of the ACL created in Step 2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For vlan-range, specify the VLAN that the switches and hosts are in. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Specify static to treat implicit denies in the ARP ACL as explicit denies and to drop packets that do not match any previous clauses in the ACL. DHCP bindings are not used. If you do not specify this keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL. ARP packets containing only IP-to-MAC address bindings are compared against the ACL. Packets are permitted only if the access list permits them.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 7**  
`interface interface-id`  
Specifies Switch A interface that is connected to Switch B, and enters the interface configuration mode.

**Step 8**  
`no ip arp inspection trust`  
Configures Switch A interface that is connected to Switch B as untrusted. By default, all interfaces are untrusted. 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 9**  
`end`  
Returns to privileged EXEC mode.

**Step 10**  
Use the following show commands:  
- `show arp access-list acl-name`  
- `show ip arp inspection vlan vlan-range`  
- `show ip arp inspection interfaces`  
Verifies your entries.

**Step 11**  
`show running-config`  
**Example:**  
`Device# show running-config`  
Verifies your entries.
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.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>show cdp neighbors</td>
<td>Verify the connection between the switches.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)#show cdp neighbors</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enable dynamic ARP inspection on a per-VLAN basis. By default, dynamic ARP inspection is disabled on all VLANs. For vlan-range, specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. Specify the same VLAN ID for both switches.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Specifies the interface connected to the other switch, and enter interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Verifies the dynamic ARP inspection configuration on interfaces.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Verifies the dynamic ARP inspection configuration on VLAN.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Verifies the DHCP bindings.</td>
<td></td>
</tr>
</tbody>
</table>
Limiting the Rate of Incoming ARP Packets

The switch CPU performs dynamic ARP inspection validation checks; therefore, the number of incoming ARP packets is rate-limited to prevent a denial-of-service attack.

When the rate of incoming ARP packets exceeds the configured limit, the switch places the port in the error-disabled state. The port remains in that state until you enable error-disabled recovery so that ports automatically emerge from this state after a specified timeout period.

Note

Unless you configure a rate limit on an interface, changing the trust state of the interface also changes its rate limit to the default value for that trust state. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed. If you enter the `no ip arp inspection limit` interface configuration command, the interface reverts to its default rate limit.

Follow these steps to limit the rate of incoming ARP packets. This procedure is optional.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 11</strong> show ip arp inspection statistics vlan vlan-range</td>
<td>Checks the dynamic ARP inspection statistics on VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# show ip arp inspection statistics vlan 1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 12</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 13</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the interface to be rate-limited, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip arp inspection limit {rate pps [burst interval seconds]</td>
<td>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.</td>
</tr>
<tr>
<td>none}</td>
<td>The keywords have these meanings:</td>
</tr>
<tr>
<td></td>
<td>• For <strong>rate pps</strong>, specify an upper limit for the number of incoming packets processed per second. The range is 0 to 2048 pps.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <strong>burst interval seconds</strong>, 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.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>rate none</strong>, specify no upper limit for the rate of incoming ARP packets that can be processed.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> Use the following commands:</td>
<td>(Optional) Enables error recovery from the dynamic ARP inspection error-disabled state, and configure the dynamic ARP inspection recover mechanism variables.</td>
</tr>
<tr>
<td>• errdisable detect cause arp-inspection</td>
<td></td>
</tr>
<tr>
<td>• errdisable recovery cause arp-inspection</td>
<td></td>
</tr>
<tr>
<td>• errdisable recovery interval <em>interval</em></td>
<td>By default, recovery is disabled, and the recovery interval is 300 seconds.</td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>For <strong>interval interval</strong>, specify the time in seconds to recover from the error-disabled state. The range is 30 to 86400.</td>
</tr>
<tr>
<td><strong>Step 8</strong> Use the following show commands:</td>
<td>Verifies your settings.</td>
</tr>
<tr>
<td>• show ip arp inspection interfaces</td>
<td></td>
</tr>
<tr>
<td>• show errdisable recovery</td>
<td></td>
</tr>
</tbody>
</table>
Performing Dynamic ARP Inspection Validation Checks

Dynamic ARP inspection intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. You can configure the switch to perform additional checks on the destination MAC address, the sender and target IP addresses, and the source MAC address.

Follow these steps to perform specific checks on incoming ARP packets. This procedure is optional.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  
  enable
  
  **Example:**
  
  Device> enable

  Enables privileged EXEC mode.

  - Enter your password if prompted.

| **Step 2**
  
  configure terminal
  
  **Example:**
  
  Device# configure terminal

  Enters global configuration mode.

| **Step 3**
  
  ip arp inspection validate {src-mac} {dst-mac} [ip]

  Performs a specific check on incoming ARP packets. By default, no checks are performed.

  The keywords have these meanings:

  - For src-mac, check the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

  - For dst-mac, check the destination MAC address in the Ethernet header against the target MAC address in 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 ip, check the IP addresses in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with invalid IP addresses are classified as invalid and are dropped.

Verifies your entries.

(Optional) Saves your entries in the configuration file.
### Command or Action | Purpose
--- | ---
| | • For **dst-mac**, check the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.
| | • For **ip**, check the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

You must specify at least one of the keywords. Each command overrides the configuration of the previous command; that is, if a command enables src and dst mac validations, and a second command enables IP validation only, the src and dst mac validations are disabled as a result of the second command.

| Step 4 | exit | Returns to privileged EXEC mode. |
| Step 5 | show ip arp inspection vlan *vlan-range* | Verifies your settings. |
| Step 6 | show running-config | Verifies your entries. |
| **Example:** | Device# show running-config |
| Step 7 | copy running-config startup-config | (Optional) Saves your entries in the configuration file. |
| **Example:** | Device# copy running-config startup-config |

### Monitoring DAI

To monitor DAI, use the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip arp inspection statistics</td>
<td>Clears dynamic ARP inspection statistics.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>show ip arp inspection statistics [vlan vlan-range]</code></td>
<td>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).</td>
</tr>
<tr>
<td><code>clear ip arp inspection log</code></td>
<td>Clears the dynamic ARP inspection log buffer.</td>
</tr>
<tr>
<td><code>show ip arp inspection log</code></td>
<td>Displays the configuration and contents of the dynamic ARP inspection log buffer.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show arp access-list [acl-name]</code></td>
<td>Displays detailed information about ARP ACLs.</td>
</tr>
<tr>
<td><code>show ip arp inspection interfaces [interface-id]</code></td>
<td>Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.</td>
</tr>
<tr>
<td><code>show ip arp inspection vlan vlan-range</code></td>
<td>Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN. If no VLANs are specified or if a range is specified, displays information only for VLANs with dynamic ARP inspection enabled (active).</td>
</tr>
</tbody>
</table>

### Additional References

**Error Message Decoder**

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

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

Technical Assistance

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

Feature Information for Dynamic ARP Inspection

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature. Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

**Table 56: Feature Information for Dynamic ARP Inspection**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic ARP Inspection</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. 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.</td>
</tr>
</tbody>
</table>
CHAPTER 21

Configuring IPv6 First Hop Security

- Prerequisites for First Hop Security in IPv6, on page 359
- Restrictions for First Hop Security in IPv6, on page 359
- Information about First Hop Security in IPv6, on page 360
- How to Configure an IPv6 Snooping Policy, on page 361
- How to Attach an IPv6 Snooping Policy to an Interface, on page 363
- How to Attach an IPv6 Snooping Policy to a Layer 2 EtherChannel Interface, on page 364
- How to Attach an IPv6 Snooping Policy to VLANs Globally, on page 365
- How to Configure the IPv6 Binding Table Content, on page 366
- How to Configure an IPv6 Neighbor Discovery Inspection Policy, on page 367
- How to Configure an IPv6 Router Advertisement Guard Policy, on page 371
- How to Configure an IPv6 DHCP Guard Policy, on page 375
- How to Configure IPv6 Source Guard, on page 380
- How to Configure IPv6 Prefix Guard, on page 383
- Configuration Examples for IPv6 First Hop Security, on page 385
- Feature Information for IPv6 First Hop Security, on page 386

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

- 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.
- By default, a snooping policy has a security-level of guard. When such a snooping policy is configured on an access switch, external IPv6 Router Advertisement (RA) or Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server packets are blocked, even though the uplink port facing the router or DHCP
server/relay is configured as a trusted port. To allow IPv6 RA or DHCPv6 server messages, do the following:

- Apply an IPv6 RA-guard policy (for RA) or IPv6 DHCP-guard policy (for DHCP server messages) on the uplink port.
- Configure a snooping policy with a lower security-level, for example glean or inspect. However; configuring a lower security level is not recommended with such a snooping policy, because benefits of First Hop security features are not effective.

**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, an EtherChannel 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 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.
- 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.

**Note**

Effective Cisco IOS XE Release 16.3.1, ND Inspection functionality, IPv6 Snooping Policy, and IPv6 FHS Binding Table Content are supported through Switch Integrated Security Feature (SISF)-based Device Tracking. For more information, see Configuring SISF based device tracking section of the Software Configuration Guide.

- 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.

- 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.

### How to Configure an IPv6 Snooping Policy

The IPv6 Snooping Policy feature has been deprecated. Although the commands are visible on the CLI and you can configure them, we recommend that you use the Switch Integrated Security Feature (SISF)-based Device Tracking feature instead.

Beginning in privileged EXEC mode, follow these steps to configure IPv6 Snooping Policy:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Examples:</td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td>Creates a snooping policy and enters IPv6 Snooping Policy Configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables data address gleaning, validates messages against various criteria, specifies the security level for messages.</td>
</tr>
<tr>
<td><code>ipv6 snooping policy policy-name</code></td>
<td>Examples:</td>
</tr>
<tr>
<td><code>Device(config)# ipv6 snooping policy example_policy</code></td>
<td>(Optional) <code>default</code>—Sets all to default options.</td>
</tr>
<tr>
<td></td>
<td>(Optional) `device-role {node</td>
</tr>
<tr>
<td></td>
<td>(Optional) <code>limit address-count value</code>—Limits the number of addresses allowed per target.</td>
</tr>
<tr>
<td></td>
<td>(Optional) <code>no</code>—Negates a command or sets it to defaults.</td>
</tr>
<tr>
<td></td>
<td>(Optional) `protocol {dhcp</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>analysis. The default, is dhcp and ndp. To change the default, use the no protocol command.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) security-level {glean</td>
<td>guard</td>
</tr>
<tr>
<td>glean — Gleans addresses from messages and populates the binding table without any verification.</td>
<td></td>
</tr>
<tr>
<td>guard — Gleans addresses and inspects messages. In addition, it rejects RA and DHCP server messages. This is the default option.</td>
<td></td>
</tr>
<tr>
<td>inspect — Gleans addresses, validates messages for consistency and conformance, and enforces address ownership.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) tracking {disable</td>
<td>enable} — Overrides the default tracking behavior and specifies a tracking option.</td>
</tr>
<tr>
<td>• (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.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-ipv6-snooping)# exit</td>
</tr>
<tr>
<td>Exits configuration modes to Privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>show ipv6 snooping policy policy-name</td>
</tr>
<tr>
<td>Example:</td>
<td>Device#show ipv6 snooping policy example_policy</td>
</tr>
<tr>
<td>Displays the snooping policy configuration.</td>
<td></td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface Interface_type stack/module/port</code></td>
<td>Specifies an interface type and identifier; enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# interface gigabitethernet 1/1/4</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>switchport</code></td>
<td>Enters the Switchport mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-if)# switchport</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>`ipv6 snooping [attach-policy policy_name [vlan vlan_id</td>
<td>add vlan_ids</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface range Interface_name</td>
<td>Specifies the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# interface range Po11</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 snooping [attach-policy policy_name [vlan vlan_ids</td>
<td>add vlan_ids</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if-range)# ipv6 snooping attach-policy example_policy</td>
<td></td>
</tr>
</tbody>
</table>

Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 snooping attach-policy example_policy vlan 222,223,224</code></td>
<td>Attaches the IPv6 Snooping policy to the specified VLANs across all switch and stack interfaces. The default policy is attached if the <code>attach-policy</code> option is not used. The default policy is, security-level <code>guard</code>, device-role <code>node</code>, protocol <code>ndp</code> and <code>dhcp</code>.</td>
</tr>
</tbody>
</table>

**Step 4**

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><code>vlan configuration vlan_list</code></td>
<td>Specifies the VLANs to which the IPv6 Snooping policy will be attached; enters the VLAN interface configuration mode.</td>
</tr>
<tr>
<td><code>ipv6 snooping [attach-policy policy_name]</code></td>
<td>attach-policy example_policy</td>
</tr>
<tr>
<td><code>do show running-config interface portchannel_interface_name</code></td>
<td>Verifies that the policy is attached to the specified VLANs without exiting the interface configuration mode.</td>
</tr>
</tbody>
</table>

#### 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:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><code>vlan configuration vlan_list</code></td>
<td>Specifies the VLANs to which the IPv6 Snooping policy will be attached; enters the VLAN interface configuration mode.</td>
</tr>
<tr>
<td><code>ipv6 snooping [attach-policy policy_name]</code></td>
<td>Attaches the IPv6 Snooping policy to the specified VLANs across all switch and stack interfaces. The default policy is attached if the <code>attach-policy</code> option is not used. The default policy is, security-level <code>guard</code>, device-role <code>node</code>, protocol <code>ndp</code> and <code>dhcp</code>.</td>
</tr>
<tr>
<td><code>do show running-config</code></td>
<td>Verifies that the policy is attached to the specified VLANs without exiting the interface configuration mode.</td>
</tr>
</tbody>
</table>
How to Configure the IPv6 Binding Table Content

Beginning in privileged EXEC mode, follow these steps to configure IPv6 Binding Table Content:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | configure terminal  
Example:  
Device# configure terminal | Enters the global configuration mode. |
| Step 2 | [no] ipv6 neighbor binding [vlan vlan-id | Adds a static entry to the binding table database. |

```
interface interface_type
stack/module/port hw_address
[reachable-lifetime value [seconds | default | infinite] | [tracking] [default | disable] [reachable-lifetime value [seconds | default | infinite] | [enable [reachable-lifetime value [seconds | default | infinite] | [retry-interval [seconds | default | infinite] | [tracking] [default | disable] [retry-interval [seconds | default | infinite] }
```

Example:  
Device(config)# ipv6 neighbor binding

| Step 3 | [no] ipv6 neighbor binding max-entries number [mac-limit number] | Specifies the maximum number of entries that are allowed to be inserted in the binding table cache. |

```
port-limit number | mac-limit number | vlan-limit number [
mac-limit number] | [port-limit number
mac-limit number] ] ] ]
```

Example:  
Device(config)# ipv6 neighbor binding max-entries 30000

| Step 4 | ipv6 neighbor binding logging  
Example:  
Device(config)# ipv6 neighbor binding logging | Enables the logging of binding table main events. |

| Step 5 | exit  
Example:  
Device(config)# exit | Exits global configuration mode, and places the router in privileged EXEC mode. |

| Step 6 | show ipv6 neighbor binding  
Example:  
Device# show ipv6 neighbor binding | 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>[no]ipv6 nd inspection policy policy-name</td>
<td>Specifies the ND inspection policy name and enters ND Inspection Policy configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ipv6 nd inspection policy example_policy</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>device-role {host</td>
<td>switch}</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-nd-inspection)# device-role switch</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>limit address-count value</td>
<td>Enter 1–10,000.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-nd-inspection)# limit address-count 1000</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>tracking {enable [reachable-lifetime {value</td>
<td>infinite}]</td>
</tr>
<tr>
<td>Example:</td>
<td>disable [stale-lifetime {value</td>
<td>infinite}]}</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>trusted-port</td>
<td>Configures a port to become a trusted port.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-nd-inspection)# trusted-port</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>validate source-mac</td>
<td>Checks the source media access control (MAC) address against the link-layer address.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-nd-inspection)# validate source-mac</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>no {device-role</td>
<td>limit address-count</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device (config-nd-inspection)# no validate source-mac</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 9**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>default {device-role</td>
<td>limit address-count</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device (config-nd-inspection)# default limit address-count</td>
<td></td>
</tr>
</tbody>
</table>

**Step 10**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>do show ipv6 nd inspection policy policy_name</td>
<td>Verifies the ND Inspection Configuration without exiting ND inspection configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device (config-nd-inspection)# do show ipv6 nd inspection policy example_policy</td>
<td></td>
</tr>
</tbody>
</table>

### 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:

**Procedure**

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

| Step 2 |         |
| Interface Interface_type stack/module/port | Specifies an interface type and identifier; enters the interface configuration mode. |
| Example: |         |
| Device(config)# interface gigabitethernet 1/1/4 |         |

<p>| Step 3 | Attach 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. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd inspection [attach-policy policy_name [vlan vlan_ids</td>
<td>add vlan_ids</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ipv6 nd inspection attach-policy example_policy</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ipv6 nd inspection attach-policy example_policy vlan</td>
<td></td>
</tr>
</tbody>
</table>
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:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface range Interface_name</td>
<td>Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# interface Po11</td>
<td></td>
</tr>
<tr>
<td>Tip</td>
<td>Enter the do show interfaces summary command for quick reference to interface names and types.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 nd inspection [attach-policy policy_name [vlan {vlan_ids</td>
<td>add vlan_ids</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if-range)# ipv6 nd inspection attach-policy example_policy</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td>Device(config-if-range)# ipv6 nd inspection attach-policy example_policy</td>
<td></td>
</tr>
</tbody>
</table>
### 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:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
*configure terminal*  
**Example:**  
Device# configure terminal                                                        | Enters the global configuration mode.                                                                                                                                                           |
| **Step 2**  
*vlan configuration* *vlan_list*  
**Example:**  
Device(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 policy_name*  
**Example:**  
Device(config-vlan-config)#ipv6 nd inspection attach-policy example_policy          | 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 *host*, no drop-unsecure, limit address-count disabled, sec-level minimum is disabled, tracking is disabled, no trusted-port, no validate source-mac.                                      |
| **Step 4**  
*do show running-config*  
**Example:**  
Device#(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:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>[no]ipv6 nd raguard policy <em>policy-name</em></td>
<td>Specifies the RA Guard policy name and enters RA Guard Policy configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ipv6 nd raguard policy <em>example_policy</em></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>[no]device-role {host</td>
<td>monitor</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-nd-raguard)# device-role switch</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>[no]hop-limit {maximum</td>
<td>minimum} <em>value</em></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-nd-raguard)# hop-limit maximum 33</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 5    | `managed-config-flag {off | on}` | Enables filtering of Router Advertisement messages by the Managed Address Configuration, or "M" flag field. A rogue 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.  
**On**—Accepts and forwards RA messages with an M value of 1, blocks those with 0.  
**Off**—Accepts and forwards RA messages with an M value of 0, blocks those with 1. |
|       | Example:  
Device(config-nd-raguard)# managed-config-flag on |         |
| 6    | `match {ipv6 access-list list | ra prefix-list list}` | Matches a specified prefix list or access list. |
|       | Example:  
Device(config-nd-raguard)# match ipv6 access-list example_list |         |
| 7    | `other-config-flag {on | off}` | Enables filtering of Router Advertisement messages by the Other Configuration, or "O" flag field. A rogue 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.  
**On**—Accepts and forwards RA messages with an O value of 1, blocks those with 0.  
**Off**—Accepts and forwards RA messages with an O value of 0, blocks those with 1. |
|       | Example:  
Device(config-nd-raguard)# other-config-flag on |         |
| 8    | `router-preference maximum {high | medium | low}` | Enables filtering of Router Advertisement messages by the Router Preference flag. If not configured, this filter is disabled.  
  • **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. |
|       | Example:  
Device(config-nd-raguard)# router-preference maximum high |         |
| 9    | `trusted-port` | When configured as a trusted port, all attached devices are trusted, and no further message verification is performed. |
|       | Example:  
Device(config-nd-raguard)# trusted-port |         |
| 10   | `default {device-role | hop-limit {maximum | minimum} | managed-config-flag | match` | Restores a command to its default value. |
### 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:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface Interface_type stack/module/port</td>
<td>Specifies an interface type and identifier; enters the interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# interface gigabitethernet 1/1/4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ipv6 nd raguard [attach-policy policy_name [vlan vlan_ids</td>
<td>add vlan_ids</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# ipv6 nd raguard attach-policy example_policy</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td>Device(config-if)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td>Device(config-if)# ipv6 nd raguard vlan 222,223,224</td>
<td></td>
</tr>
</tbody>
</table>
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:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface range Interface_name</td>
<td>Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# interface Po11</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Enter the do show interfaces summary command for quick reference to interface names and types.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ipv6 nd raguard [attach-policy policy_name [vlan vlan_ids</td>
<td>add vlan_ids</td>
</tr>
<tr>
<td>Example: Device(config-if-range)# ipv6 nd raguard attach-policy example_policy</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Device(config-if-range)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Device(config-if-range)#ipv6 nd raguard vlan 222, 223, 224</td>
<td></td>
</tr>
</tbody>
</table>
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:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> vlan configuration <em>vlan_list</em></td>
<td>Specifies the VLANs to which the IPv6 RA Guard policy will be attached; enters the VLAN interface configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# vlan configuration 335</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ipv6 dhcp guard [attach-policy <em>policy_name</em>]</td>
<td>Attaches the IPv6 RA Guard policy to the specified VLANs across all switch and stack interfaces. The default policy is attached if the <em>attach-policy</em> option is not used.</td>
</tr>
<tr>
<td>Example: Device(config-vlan-config)#ipv6 nd raguard attach-policy example_policy</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> do show running-config</td>
<td>Confirms that the policy is attached to the specified VLANs without exiting the configuration mode.</td>
</tr>
<tr>
<td>Example: Device#(config-if)# do show running-config</td>
<td></td>
</tr>
</tbody>
</table>

How to Configure an IPv6 DHCP Guard Policy

Beginning in privileged EXEC mode, follow these steps to configure an IPv6 DHCP (DHCPv6) Guard policy:
# How to Configure an IPv6 DHCP Guard Policy

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>[no] ipv6 dhcp guard policy policy-name</code></td>
<td>Specifies the DHCPv6 Guard policy name and enters DHCPv6 Guard Policy configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ipv6 dhcp guard policy example_policy</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>`[no] device-role {client</td>
<td>server}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-dhcp-guard)# device-role server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>client</code>—Default value, specifies that the attached device is a client. Server messages are dropped on this port.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>server</code>—Specifies that the attached device is a DHCPv6 server. Server messages are allowed on this port.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>[no] match server access-list ipv6-access-list-name</code></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)## ipv6 access-list my_acls Device(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any Device(config-dhcp-guard)# match server access-list my_acls</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>[no] match reply prefix-list ipv6-prefix-list-name</code></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)## ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128 Device(config-dhcp-guard)# match reply prefix-list my_prefix</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

| Step 6      | [no] preference { max limit | min limit } |
|-------------|---------------------------------------------|
| Example:    | Device(config-dhcp-guard)# preference max 250 |
|             | Device(config-dhcp-guard)# preference min 150 |

**Purpose**

Configure `max` and `min` when `device-role` is `server` to filter DHCPv6 server advertisements by the server preference value. The defaults permit all advertisements.

- **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.

- **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.

<table>
<thead>
<tr>
<th>Step 7</th>
<th>[no] trusted-port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-dhcp-guard)# trusted-port</td>
</tr>
</tbody>
</table>

**Purpose**

(Optional) `trusted-port`—Sets the port to a trusted mode. No further policing takes place on the port.

**Note**

If you configure a trusted port then the device-role option is not available.

| Step 8      | default {device-role | trusted-port} |
|-------------|-------------------|
| Example:    | Device(config-dhcp-guard)# default device-role |

**Purpose**

(Optional) `default`—Sets a command to its defaults.

<table>
<thead>
<tr>
<th>Step 9</th>
<th>do show ipv6 dhcp guard policy policy_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-dhcp-guard)# do show ipv6 dhcp guard policy example_policy</td>
</tr>
</tbody>
</table>

**Purpose**

(Optional) Displays the configuration of the IPv6 DHCP guard policy without leaving the configuration submode. Omitting the `policy_name` 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
do show ipv6 dhcp guard policy example_policy
```

---

Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)
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:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface Interface_type stack/module/port</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# interface gigabitethernet 1/1/4</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ipv6 dhcp guard [attach-policy policy_name [vlan {vlan_ids</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# ipv6 dhcp guard attach-policy example_policy</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# ipv6 dhcp guard vlan 222, 223,224</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>do show running-config interface Interface_type stack/module/port</td>
</tr>
<tr>
<td>Example:</td>
<td>Device#(config-if)# do show running-config gig 1/1/4</td>
</tr>
</tbody>
</table>

The default policy is attached if the **attach-policy** option is not used.
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:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface range Interface_name</td>
<td>Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# interface Po11</td>
<td></td>
</tr>
<tr>
<td>Tip</td>
<td>Enter the do show interfaces summary command for quick reference to interface names and types.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 dhcp guard [attach-policy policy_name [vlan vlan_ids</td>
<td>add vlan_ids</td>
</tr>
<tr>
<td></td>
<td>vlan_ids</td>
<td>add vlan_ids</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-if-range)# ipv6 dhcp guard attach-policy example_policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if-range)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if-range)#ipv6 dhcp guard vlan 222, 223,224</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>do show running-config interfaceportchannel_interface_name</td>
<td>Confirms that the policy is attached to the specified interface without exiting the configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device#(config-if-range)# do show running-config int po11</td>
<td></td>
</tr>
</tbody>
</table>
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:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>vlan configuration vlan_list</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# vlan configuration 334</td>
</tr>
<tr>
<td></td>
<td>Specifies the VLANs to which the IPv6 Snooping policy will be attached; enters the VLAN interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ipv6 dhcp guard [attach-policy policy_name]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-vlan-config)#ipv6 dhcp guard attach-policy example_policy</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>do show running-config</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device#(config-if)# do show running-config</td>
</tr>
<tr>
<td></td>
<td>Confirms that the policy is attached to the specified VLANs without exiting the configuration mode.</td>
</tr>
</tbody>
</table>

---

How to Configure IPv6 Source Guard

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters the global configuration mode.</td>
</tr>
</tbody>
</table>
### Purpose

#### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>[no] ipv6 source-guard policy policy_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config)# ipv6 source-guard policy example_policy</td>
</tr>
</tbody>
</table>

- Specifies the IPv6 Source Guard policy name and enters IPv6 Source Guard policy configuration mode.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>[deny global-autoconf] [permit link-local] [default{...}] [exit [no{...}]]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-sisf-sourceguard)# deny global-autoconf</td>
</tr>
</tbody>
</table>

- (Optional) Defines the IPv6 Source Guard policy.
  - **deny global-autoconf**—Denies data traffic from auto-configured global addresses. This is useful when all global addresses on a link are DHCP-assigned and the administrator wants to block hosts with self-configured addresses to send traffic.
  - **permit link-local**—Allows all data traffic that is sourced by a link-local address.

**Note**

- Trusted option under source guard policy is not supported.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-sisf-sourceguard)# end</td>
</tr>
</tbody>
</table>

- Exits out of IPv6 Source Guard policy configuration mode.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>show ipv6 source-guard policy policy_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device# show ipv6 source-guard policy example_policy</td>
</tr>
</tbody>
</table>

- Shows the policy configuration and all the interfaces where the policy is applied.

### What to do next

Apply the IPv6 Source Guard policy to an interface.

### How to Attach an IPv6 Source Guard Policy to an Interface

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
</tbody>
</table>
### How to attach an IPv6 Source Guard Policy to a Layer 2 EtherChannel Interface

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies an interface type and port number and places the switch in the port channel configuration mode.</td>
</tr>
<tr>
<td><code>interface port-channel port-channel-number</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device (config)# interface Po4</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Attaches the IPv6 Source Guard policy to the interface. The default policy is attached if the <code>attach-policy</code> option is not used.</td>
</tr>
<tr>
<td><code>ipv6 source-guard [attach-policy &lt;policy_name&gt; ]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-if)# ipv6 source-guard attach-policy example_policy</code></td>
<td></td>
</tr>
</tbody>
</table>
### How to Configure IPv6 Prefix Guard

**Note**

To allow routing protocol control packets sourced by a link-local address when prefix guard is applied, enable the permit link-local command in the source-guard policy configuration mode.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
- Enter your password if prompted.  

**Example:**

Device> enable |
| **Step 2** | configure terminal | Enters global configuration mode.  

**Example:**

Device# configure terminal |
| **Step 3** | [no] ipv6 source-guard policy source-guard-policy | Defines an IPv6 source-guard policy name and enters switch integrated security features source-guard policy configuration mode.  

**Example:**

Device (config)# ipv6 source-guard policy my_snooping_policy |
| **Step 4** | [no] validate address | Enables IPv6 source guard to perform the IPv6 prefix-guard operation.  

**Example:**

Device (config-sisf-sourceguard)# no validate address |
| **Step 5** | validate prefix | Enables IPv6 source guard to perform the IPv6 prefix-guard operation.  

**Example:**

Device (config-sisf-sourceguard)# validate prefix |
### How to Attach an IPv6 Prefix Guard Policy to an Interface

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface Interface_type stack/module/port</td>
<td>Specifies an interface type and identifier; enters the interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# interface gigabitethernet 1/1/4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ipv6 source-guard attach-policy policy_name</td>
<td>Attaches the IPv6 Source Guard policy to the interface. The default policy is attached if the attach-policy option is not used.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# ipv6 source-guard attach-policy example_policy</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show ipv6 source-guard policy policy_name</td>
<td>Shows the policy configuration and all the interfaces where the policy is applied.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# show ipv6 source-guard policy example_policy</td>
<td></td>
</tr>
</tbody>
</table>
How to attach an IPv6 Prefix Guard Policy to a Layer 2 EtherChannel Interface

Procedure

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

| **Step 2**        | Enters the global configuration mode. |
| configure terminal| |
| Example:          | |
| Device# configure terminal | |

| **Step 3**        | Specifies an interface type and port number and places the switch in the port channel configuration mode. |
| interface port-channel port-channel-number | |
| Example:          | |
| Device (config)# interface Po4 | |

| **Step 4**        | Attaches the IPv6 Source Guard policy to the interface. The default policy is attached if the attach-policy option is not used. |
| ipv6 source-guard [attach-policy <policy_name> ] | |
| Example:          | |
| Device(config-if)# ipv6 source-guard attach-policy example_policy | |

| **Step 5**        | Shows the policy configuration and all the interfaces where the policy is applied. |
| show ipv6 source-guard policy policy_name | |
| Example:          | |
| Device(config-if)# show ipv6 source-guard policy example_policy | |

Configuration Examples for IPv6 First Hop Security

Examples: How to attach an IPv6 Source Guard Policy to a Layer 2 EtherChannel Interface

The following example shows how to attach an IPv6 Source Guard Policy to a Layer 2 EtherChannel Interface:

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch(config-sisf-sourceguard)# validate address
Switch(config-sisf-sourceguard)# exit
Switch(config)# interface Po4
Switch(config)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL
Switch(config-if)# exit
Switch(config)#
```
Examples: How to attach an IPv6 Prefix Guard Policy to a Layer 2 EtherChannel Interface

The following example shows how to attach an IPv6 Prefix Guard Policy to a Layer 2 EtherChannel Interface:

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch (config-sisf-sourceguard)# no validate address
Switch((config-sisf-sourceguard)# validate prefix
Switch(config)# interface Po4
Switch(config-if)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL
```

Feature Information for IPv6 First Hop Security

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 First Hop Security</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>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, an EtherChannel 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 IPv6 Snooping Policy feature has been deprecated. Although the commands are visible on the CLI and you can configure them, we recommend that you use the Switch Integrated Security Feature (SISF)-based Device Tracking feature instead.</td>
</tr>
</tbody>
</table>

To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
CHAPTER 22

Configuring SISF-Based Device Tracking

- Information About SISF-Based Device Tracking, on page 387
- How to Configure SISF-Based Device Tracking, on page 390
- Configuration Examples for SISF-Based Device Tracking, on page 398
- Feature History and Information for SISF-Based Device Tracking, on page 403

Information About SISF-Based Device Tracking

Overview of SISF-Based Device Tracking

The Switch Integrated Security Features based (SISF-based) device tracking feature is part of the suite of first-hop security features.

The main role of the feature is to track the presence, location, and movement of end-nodes in the network. SISF snoops traffic received by the switch, extracts device identity (MAC and IP address), and stores them in a binding table. Many features, such as, IEEE 802.1X, web authentication, Cisco TrustSec and LISP etc., depend on the accuracy of this information to operate properly.

SISF-based device tracking supports both IPv4 and IPv6.

Even with the introduction of SISF-based device tracking, the legacy device tracking CLI (IP Device Tracking (IPDT) and IPv6 Snooping CLI) continues to be available. When you bootup the switch, the set of commands that is available depends on existing configuration, and only one of the following is available:

- SISF-based device tracking CLI, or
- IPDT and IPv6 Snooping CLI

Note

The IPDT and IPv6 Snooping commands are deprecated, but continue to be available. We recommend that you upgrade to SISF-based device tracking.

If you are using the IPDT and IPv6 Snooping CLI and want to migrate to SISF-based device tracking, see Migrating from legacy IPDT and IPv6 Snooping to SISF-Based Device Tracking, for more information.

SISF-based device tracking can be enabled manually (by using device-tracking commands), or programmatically (which is the case when providing device tracking services to other features).
Options to Enable SISF-Based Device Tracking

SISF-Based device tracking is disabled by default.

You can enable it by defining a device tracking policy and attaching the policy to a specific target.

**Note**
The target could be an interface or a VLAN.

**Manually Enabling SISF-Based Device Tracking**

- **Option 1**: Apply the `default` device tracking policy to a target.
  
Enter the `device-tracking` command in the interface configuration mode or in the VLAN configuration mode. The system then attaches the `default` policy to the interface or VLAN.

  **Note**
The `default` policy is a built-in policy with default settings; you cannot change any of the attributes of the `default` policy. In order to be able to configure device tracking policy attributes you must create a custom policy. See **Option 2: Create a custom policy with custom settings**.

- **Option 2**: Create a custom policy with custom settings.
  
Enter the device-tracking policy command in global configuration mode and enter a custom policy name. The system creates a policy with the name you specify. You can then configure the available settings, in the device tracking configuration mode (config-device-tracking), and attach the policy to a specified target.

**Programmatically Enabling SISF-Based Device Tracking**

Some features rely on device tracking and utilize the trusted database of binding entries that SISF-based device tracking builds and maintains. These features, also called device tracking clients, enable device tracking programmatically (create and attach the device tracking policy).

**Note**
The exceptions here are IEEE 802.1X, web authentication, Cisco TrustSec, and IP Source Guard (IPSG) - they also rely on device tracking, but they do not enable it. For these device tracking clients, you must enter the `ip dhcp snooping vlan vlan` command, to programmatically enable device tracking on a particular target.

Note the following about programmatically enabling SISF-based device tracking:

- A device tracking client **requires** device tracking to be enabled.
  
  There are several device tracking clients, therefore, multiple programmatic policies could be created. The settings of each policy differ depending on the device tracking client that creates the policy.

- The policy that is created, and its settings, are system-defined.
Configurable policy attributes are available in the device tracking configuration mode (config-device-tracking) and vary from one release to another. If you try to modify an attribute that is not configurable, the configuration change is rejected and an error message is displayed.

For release-specific information about programmatically created policies, see *Programmatically Enabling SISF-Based Device Tracking in Cisco IOS XE* `<release name> <release number>` in the required version of the document.

## Migrating from Legacy IPDT and IPv6 Snooping to SISF-Based Device Tracking

Based on the legacy configuration that exists on your device, the `device-tracking upgrade-cli` command upgrades your CLI differently. Consider the following configuration scenarios and the corresponding migration results before you migrate your existing configuration.

### Note
You cannot configure a mix of the old IPDT and IPv6 snooping CLI with the SISF-based device tracking CLI.

### Only IPDT Configuration Exists

If your device has only IPDT configuration, running the `device-tracking upgrade-cli` command converts the configuration to use the new SISF policy that is created and attached to the interface. You can then update this SISF policy.

If you continue to use the legacy commands, this restricts you to operate in a legacy mode where only the legacy IPDT and IPv6 snooping commands are available on the device.

### Only IPv6 Snooping Configuration Exists

On a device with existing IPv6 snooping configuration, the old IPv6 Snooping commands are available for further configuration. The following options are available:

- (Recommended) Use the `device-tracking upgrade-cli` command to convert all your legacy configuration to the new SISF-based device tracking commands. After conversion, only the new device tracking commands will work on your device.

- Use the legacy IPv6 Snooping commands for your future configuration and do not run the `device-tracking upgrade-cli` command. With this option, only the legacy IPv6 Snooping commands are available on your device, and you cannot use the new SISF-based device tracking CLI commands.

### Both IPDT and IPv6 Snooping Configuration Exist

On a device that has both legacy IPDT configuration and IPv6 snooping configuration, you can convert legacy commands to the SISF-based device tracking CLI commands. However, note that only one snooping policy can be attached to an interface, and the IPv6 snooping policy parameters override the IPDT settings.
If you do not migrate to the new SISF-based commands and continue to use the legacy IPv6 snooping or IPDT commands, your IPv4 device tracking configuration information may be displayed in the IPv6 snooping commands, as the SISF-based device tracking feature handles both IPv4 and IPv6 configuration. To avoid this, we recommend that you convert your legacy configuration to SISF-based device tracking commands.

---

**Note**

**No IPDT or IPv6 Snooping Configuration Exists**

If your device has no legacy IP Device Tracking or IPv6 Snooping configurations, you can use only the new SISF-based device tracking commands for all your future configuration. The legacy IPDT commands and IPv6 snooping commands are not available.

---

**How to Configure SISF-Based Device Tracking**

**Manually Enabling SISF-Based Device Tracking**

**Applying the Default Device Tracking Policy to a Target**

Beginning in privileged EXEC mode, follow these steps to apply the default device tracking policy to an interface or VLAN:

**Procedure**

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

**Step 2**

Specify an interface or a VLAN

- interface interface
- vlan configuration vlan_list

**Example:**

Device(config)# interface gigabitethernet 1/1/4
OR
Device(config)# vlan configuration 333

**interface type number**—Specifies the interface and enters the interface configuration mode. The device tracking policy will be attached to the specified interface.

**vlan configuration vlan_list**—Specifies the VLANs and enters the VLAN feature configuration mode. The device tracking policy will be attached to the specified VLAN.

**Step 3**

**device-tracking**

**Example:**

Device(config-if)# device-tracking
OR
Device(config-vlan-config)# device-tracking

Enables SISF-based device tracking and attaches the default policy it to the interface or VLAN.

The default policy is a built-in policy with default settings; none of the attributes of the default policy can be changed.
Creating a Custom Device Tracking Policy with Custom Settings

Beginning in privileged EXEC mode, follow these steps to create and configure a device tracking policy:

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>[no] device-tracking policy policy-name</td>
<td>Creates the policy and enters the device-tracking configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# device-tracking policy example_policy</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>[data-glean</td>
<td>default</td>
</tr>
<tr>
<td>Example: Device (config-device-tracking)# destination-glean log-only</td>
<td></td>
</tr>
<tr>
<td><strong>(Optional) data-glean</strong>—Enables learning of addresses from a data packet snooped from a source inside the network and populates the binding table with the data traffic source address. Enter one of these options:</td>
<td></td>
</tr>
<tr>
<td>• log-only—Generates a syslog message upon data packet notification</td>
<td></td>
</tr>
<tr>
<td>• recovery—Uses a protocol to enable binding table recovery. Enter NDP or DHCP.</td>
<td></td>
</tr>
<tr>
<td><strong>(Optional) default</strong>—Sets the policy attribute to its default value. You can set</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>• (Optional) <strong>destination-glean</strong>—Populates the binding table by gleaning data traffic destination address. Enter one of these options:</td>
<td></td>
</tr>
<tr>
<td>• log-only—Generates a syslog message upon data packet notification</td>
<td></td>
</tr>
<tr>
<td>• recovery—Uses a protocol to enable binding table recovery. Enter <strong>DHCP</strong>.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>device-role</strong>—Sets the role of the device attached to the port. It can be a node or a switch. Enter one of these options:</td>
<td></td>
</tr>
<tr>
<td>• node—Configures the attached device as a node. This is the default option.</td>
<td></td>
</tr>
<tr>
<td>• switch—Configures the attached device as a switch.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>distribution-switch</strong>—Although visible on the CLI, this option is not supported. Any configuration settings you make will not take effect.</td>
<td></td>
</tr>
<tr>
<td>• <strong>exit</strong>—Exits the device-tracking policy configuration mode.</td>
<td></td>
</tr>
<tr>
<td>• <strong>limit</strong> address-count— Specifies an address count limit per port. The range is 1 to 32000.</td>
<td></td>
</tr>
<tr>
<td>• <strong>no</strong>—Negates the command or sets it to defaults.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>prefix-glean</strong>—Enables learning of prefixes from either IPv6 Router Advertisements or from DHCP-PD. You have the following option:</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>only</strong>—Gleans only prefixes and not host addresses.</td>
<td></td>
</tr>
</tbody>
</table>
| • (Optional) **protocol**—Sets the protocol to glean; by default, all are gleaned. Enter one of these options:
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>arp [prefix-list name]</strong> — Gleans addresses in ARP packets. Optionally, enter the name of prefix-list that is to be matched.</td>
<td></td>
</tr>
<tr>
<td><strong>dhcp4 [prefix-list name]</strong> — Glean addresses in DHCPv4 packets. Optionally, enter the name of prefix-list that is to be matched.</td>
<td></td>
</tr>
<tr>
<td><strong>dhcp6 [prefix-list name]</strong> — Glean addresses in DHCPv6 packets. Optionally, enter the name of prefix-list that is to be matched.</td>
<td></td>
</tr>
<tr>
<td><strong>ndp [prefix-list name]</strong> — Glean addresses in NDP packets. Optionally, enter the name of prefix-list that is to be matched.</td>
<td></td>
</tr>
<tr>
<td><strong>udp [prefix-list name]</strong> — Although visible on the CLI, this option is not supported. Any configuration settings you make will not take effect.</td>
<td></td>
</tr>
<tr>
<td><strong>(Optional) security-level</strong> — Specifies the level of security enforced by the feature. Enter one of these options:</td>
<td></td>
</tr>
<tr>
<td>• <strong>glean</strong> — Gleans addresses passively.</td>
<td></td>
</tr>
<tr>
<td>• <strong>guard</strong> — Inspects and drops un-authorized messages. This is the default.</td>
<td></td>
</tr>
<tr>
<td>• <strong>inspect</strong> — Gleans and validates messages.</td>
<td></td>
</tr>
<tr>
<td><strong>(Optional) tracking</strong> — Specifies a tracking option. Enter one of these options:</td>
<td></td>
</tr>
<tr>
<td>• **disable [stale-lifetime [1-86400-seconds</td>
<td>infinite]]** — Turns off device-tracking. Optionally, you can enter the duration for which the entry is kept inactive before deletion, or keep it permanently inactive.</td>
</tr>
<tr>
<td>• **enable [reachable-lifetime [1-86400-seconds</td>
<td>infinite]]** — Turns on device-tracking.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optionally, you can enter the duration for which the entry is kept reachable, or keep it permanently reachable.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>trusted-port</strong> — Sets up a trusted port. 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.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>vpc</strong> — Although visible on the CLI, this option is not supported. Any configuration settings you make will not take effect.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> show device-tracking policy <em>policy-name</em></td>
<td>Displays the device-tracking policy configuration.</td>
</tr>
</tbody>
</table>

### What to do next

Attach the policy to an interface or VLAN.

### Attaching a Device Tracking Policy to an Interface

Beginning in privileged EXEC mode, follow these steps to attach a device tracking policy to an interface:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface <em>interface</em></td>
<td>Specifies an interface and enters the interface configuration mode.</td>
</tr>
</tbody>
</table>

*Example:

Device(config-device-tracking)# exit

Device# show device-tracking policy example_policy
Purpose
Command or Action
Step 3 [no] device-tracking attach-policy policy
name
Example:
Device(config-if)# device-tracking attach-policy example_policy

Purpose
At the device tracking policy to the
interface. Device tracking is also supported on
EtherChannels.

Note
SISF based device-tracking policies
can be disabled only if they are
custom policies. Programmatically
created policies can be removed only
if the corresponding device-tracking
client feature configuration is
removed.

Step 4 end
Example:
Device# end

Purpose
Returns to the privileged EXEC mode.

Step 5 show device-tracking policies [interface
interface]
Example:
Device# show device-tracking policies
interface gigabitethernet 1/1/4

Purpose
Displays policies that match the specified
interface type and number.

Attaching a Device Tracking Policy to a VLAN
Beginning in privileged EXEC mode, follow these steps to attach a device-tracking policy to VLANs across multiple interfaces:

Procedure
Command or Action
Step 1 configure terminal
Example:
Device# configure terminal

Purpose
Enters the global configuration mode.

Step 2 vlan configuration vlan_list
Example:
Device(config)# vlan configuration 333

Purpose
Specifies the VLANs to which the device
tracking policy will be attached; enters the
VLAN interface configuration mode.

Step 3 [no] device-tracking attach-policy policy_name
Example:

Purpose
Attaches the device tracking policy to the
specified VLANs across all switch interfaces.
Programmatically Enabling SISF-Based Device Tracking in Cisco IOS XE Fuji 16.9.x and Later Releases

**Table 58: Programmatically Enabling SISF-Based Device Tracking in Cisco IOS XE Fuji 16.9.x and Later Releases**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-vlan-config)# device-tracking attach-policy example_policy</td>
<td>SISF based device-tracking policies can be disabled only if they are custom policies. Programmatically created policies can be removed only if the corresponding device-tracking client feature configuration is removed.</td>
</tr>
</tbody>
</table>

**Step 4**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>do show device-tracking policies vlan vlan-ID</td>
<td>Verifies that the policy is attached to the specified VLAN, without exiting the VLAN interface configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Device(config-vlan-config)# do show device-tracking policies vlan 333
```
### User Options

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Policy priority is supported. Priority is determined by how the policy is created. A manually created policy has the highest priority. This enables you to apply policy settings that are different from policies that are generated programmatically.</td>
</tr>
<tr>
<td></td>
<td>• Multiple policies can be attached to the same VLAN.</td>
</tr>
<tr>
<td></td>
<td>• When multiple policies with different priorities are attached to the same VLAN, the settings of the policy with the highest priority are effective. The exceptions here are the <code>limit address-count for IPv4 per mac</code> and <code>limit address-count for IPv6 per mac</code> settings - the settings of the policy with the lowest priority are effective.</td>
</tr>
<tr>
<td></td>
<td>• The policy cannot be removed unless the device tracking client feature configuration is removed.</td>
</tr>
<tr>
<td></td>
<td>• The policy attributes cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>• You cannot change the address count limit per MAC. This refers to the <code>limit address-count for IPv4 per mac</code> and <code>limit address-count for IPv6 per mac</code> commands.</td>
</tr>
<tr>
<td></td>
<td>• In order to change a policy setting on a VLAN, create a customized device-tracking policy and attach it to the VLAN.</td>
</tr>
<tr>
<td></td>
<td>• When a device-tracking policy is attached to an interface under a VLAN, the policy settings on the interface take precedence over those on its VLAN; exceptions here are the values for <code>limit address-count for IPv4 per mac</code> and <code>limit address-count for IPv6 per mac</code>, which are aggregated from the policy on both the interface and VLAN.</td>
</tr>
</tbody>
</table>

---

### Configuring a Multi-Switch Network to Stop Creating Binding Entries from a Trunk Port

In a multi-switch network, SISF-based device tracking provides the capability to distribute binding table entries between switches running the feature. Binding entries are only created on the switches where the host appears on an access port. No entry is created for a host that appears over a trunk port. This is achieved by configuring a policy with the `trusted-port` and `device-role switch` options, and attaching it to the trunk port.

**Important**

Both, the `trusted-port`, and `device-role switch` options, must be configured in the policy.

Further, we recommended that you apply such a policy on a port facing a device, which also has SISF-based device tracking enabled.

Complete the following steps:
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>device-tracking policy policy-name</code></td>
<td>Enters the device-tracking policy configuration mode, for the specified policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# device-tracking policy</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>example_trusted_policy</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>device-role switch</code></td>
<td>Specifies the role of the device attached to the port. Default is node. Enter the <code>device-role switch</code> option to stop the creation of binding entries for the port.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-device-tracking)# device-role switch</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>trusted-port</code></td>
<td>Sets up a trusted port. 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-device-tracking)# trusted-port</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Exits the device-tracking policy configuration mode and enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-device-tracking)# end</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>interface interface</code></td>
<td>Specifies an interface and enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# interface gigabitethernet 1/0/25</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>device-tracking attach-policy policy-name</code></td>
<td>Attaches a device tracking policy to the interface or the specified VLANs on the interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-if)# device-tracking attach-policy example_trusted_policy</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuration Examples for SISF-Based Device Tracking

These examples show sample device-tracking configuration and other recommended or related configuration for certain situations.
Example: Programmatically Enabling SISF-Based Device Tracking in Cisco IOS XE Everest 16.9.x and Later Releases

The sample output in the examples show the different settings of programmatically created policies.

**Device tracking client: LISP on VLAN**

After you configure LISP, enter the `show device-tracking policy` command in privileged EXEC mode, to display the `LISP-DT-GUARD-VLAN` policy that is created and the corresponding settings.

```
Device# show device-tracking policy LISP-DT-GUARD-VLAN
Policy LISP-DT-GUARD-VLAN configuration:
    security-level guard (*)
    device-role node
    gleaning from Neighbor Discovery
    gleaning from DHCP
    gleaning from ARP
    gleaning from DHCP4
    NOT gleaning from protocol unkn
    limit address-count for IPv4 per mac 4 (*)
    limit address-count for IPv6 per mac 12 (*)
    tracking enable
Policy LISP-DT-GUARD-VLAN is applied on the following targets:
  Target Type Policy Feature Target range
  vlan 10 VLAN LISP-DT-GUARD-VLAN Device-tracking vlan all

note:
  Binding entry Down timer: 10 minutes (*)
  Binding entry Stale timer: 30 minutes (*)
```

**Device tracking client: LISP on VLAN**

After you configure LISP, enter the `show device-tracking policy` command in privileged EXEC mode, to display the `LISP-DT-GLEAN-VLAN` policy that is created and the corresponding settings:

```
Device# show device-tracking policy LISP-DT-GLEAN-VLAN
Policy LISP-DT-GLEAN-VLAN configuration:
    security-level glean (*)
    device-role node
    gleaning from Neighbor Discovery
    gleaning from DHCP
    gleaning from ARP
    gleaning from DHCP4
    NOT gleaning from protocol unkn
    limit address-count for IPv4 per mac 4 (*)
    limit address-count for IPv6 per mac 12 (*)
    tracking enable
Policy LISP-DT-GGUARD-VLAN is applied on the following targets:
  Target Type Policy Feature Target range
  vlan 10 VLAN LISP-DT-GLEAN-VLAN Device-tracking vlan all

note:
  Binding entry Down timer: 10 minutes (*)
  Binding entry Stale timer: 30 minutes (*)
```

**Device tracking client: EVPN on VLAN**

After you configure EVPN, enter the `show device-tracking policy` command in privileged EXEC mode, to display the `evpn-sisf-policy` policy that is created and the corresponding settings that are made:
Device# show device-tracking policy evpn-sisf-policy
Policy evpn-sisf-policy configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  tracking enable
Policy evpn-sisf-policy is applied on the following targets:
  Target  Type  Policy          Feature              Target range
  vlan 10  VLAN  evpn-sisf-policy  Device-tracking  vlan all

  note:
  Binding entry Down timer: 24 hours (*)
  Binding entry Stale timer:  24 hours (*)

Device tracking clients: IEEE 802.1X, Web Authentication, Cisco TrustSec, IPSG

Configure the ip dhcp snooping vlan  vlan command in global configuration mode to enable device-tracking for the IEEE 802.1X, web authentication, Cisco TrustSec, and IPSG features. Enter the show device-tracking policy command in privileged EXEC mode, to display the DT-PROGRAMMATIC policy that is created and the corresponding settings that are made:

Device# configure terminal
Device(config)# ip dhcp snooping vlan 10
Device(config)# end
Device# show device-tracking policy DT-PROGRAMMATIC
Policy DT-PROGRAMMATIC configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 1 (*)
  tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
  Target  Type  Policy          Feature              Target range
  vlan 10  VLAN  DT-PROGRAMMATIC  Device-tracking  vlan all

  note:
  Binding entry Down timer: 24 hours (*)
  Binding entry Stale timer:  24 hours (*)

Identifying the Active Policy When Multiple Policies are Applied to a Target

This example shows you how to identify the active policy when multiple policies are attached to the same VLAN.

In this example, two policies are attached to VLAN 10; LISP-DT-GUARD-VLAN is the active policy.

Device# show device-tracking policies
  Target  Type  Policy          Feature              Target range
  vlan 10  VLAN  DT-PROGRAMMATIC  Device-tracking  vlan all
  vlan 10  VLAN  LISP-DT-GUARD-VLAN  Device-tracking  vlan all

Device# show device-tracking capture-policy vlan 10
Example: Disabling IPv6 Device Tracking on a Target

By default, SISF-based device tracking supports both IPv4 and IPv6. The following configuration examples show how you can disable IPv6 device tracking if you have to:

Disabling IPv6 device tracking when the target is attached to a custom policy:

```
Device(config)# device-tracking policy example-policy
Device(config-device-tracking)# no protocol ndp
Device(config-device-tracking)# no protocol dhcp6
Device(config-device-tracking)# end
```

Disabling IPv6 device tracking when the target is attached to a programmatic policy:

In Cisco IOS XE Everest 16.6.x and Cisco IOS XE Fuji 16.8.x, you can disable IPv6 device tracking by changing the programmatic policy:

```
Device(config)# device-tracking policy DT-PROGRAMMATIC
Device(config-device-tracking)# no protocol ndp
Device(config-device-tracking)# no protocol dhcp6
Device(config-device-tracking)# end
```

In Cisco IOS XE Fuji 16.9.x and all later releases, you can disable IPv6 device tracking by attaching another customized policy to the same target:

1. Create a policy

```
Device(config)# device-tracking policy DT-noIPv6
Device(config-device-tracking)# no protocol ndp
Device(config-device-tracking)# no protocol dhcp6
Device(config-device-tracking)# tracking enable
Device(config-device-tracking)# end
```

2. Attach the policy to the required target

```
Device(config)# vlan config
Device(config)# vlan configuration 100
Device(config-vlan-config)# device-tracking attach-policy DT-noIPv6
Device(config-vlan-config)#
```

3. If you have configured LISP on the target, configure these timers, in the global configuration mode:

```
Device(config)# device-tracking binding stale-lifetime 1800
Device(config)# device-tracking binding down-lifetime 600
```

Example: Enabling IPv6 for SVI on VLAN (To Mitigate the Duplicate Address Problem)

When IPv6 is enabled in the network and a switched virtual interface (SVI) is configured on a VLAN, we recommend that you add the following to the SVI configuration. This enables the SVI to acquire a link-local
address automatically; this address is used as the source IP address of the SISF probe, thus preventing the duplicate IP address issue.

```
Device(config)# interface vlan 10
Device(config-if)# ipv6 enable
Device(config-if)# end
```

Example: Mitigating the IPv4 Duplicate Address Problem

This example shows how you can tackle the Duplicate IP Address 0.0.0.0 error message problem encountered by clients that run Microsoft Windows:

Configure the `device-tracking tracking auto-source` command in global configuration mode. This command determines the source IP and MAC address used in the Address Resolution Packet (ARP) request sent by the switch to probe a client, in order to maintain its entry in the device-tracking table. The purpose is to avoid using 0.0.0.0 as source IP address.

**Note**

Configure the `device-tracking tracking auto-source` command when a switch virtual interface (SVI) is not configured. You do not have to configure it when a SVI is configured with an IPv4 address on the VLAN.

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
</table>
| `device-tracking tracking auto-source` | • Set source to VLAN SVI if present.  
• Look for IP and MAC binding in device-tracking table from same subnet.  
• Use 0.0.0.0 | We recommend that you disable device-tracking on all trunk ports to avoid MAC flapping. |
| `device-tracking tracking auto-source override` | • Set source to VLAN SVI if present  
• Use 0.0.0.0 | Not recommended when there is no SVI.                                                     |
### Example: Avoiding a Short Device-Tracking Binding Reachable Time

When migrating from an older release, the following configuration may be present:

```plaintext
device-tracking binding reachable-time 10
```

Remove this by entering the `no` version of the command.

### Feature History and Information for SISF-Based Device Tracking

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
</table>
| `ip device tracking probe auto-source fallback 0.0.0.X 255.255.255.0` | • Set source to VLAN SVI if present.  
• Look for IP and MAC binding in device-tracking table from same subnet.  
• Compute source IP from client IP using host bit and mask provided. Source MAC is taken from the MAC address of the switchport facing the client*. | We recommend that you disable device-tracking on all trunk ports to avoid MAC flapping.  
The computed IPv4 address must not be assigned to any client or network device. |

* Depending on the client IP address, an IPv4 address has to be reserved for the source IP.

A reserved source IPv4 address = (host-ip and mask) | client-ip

- Client IP = 192.0.2.25
  - Source IP = (192.0.2.25 and 255.255.255.0) | (0.0.0.1) = 192.0.2.1

IP address 192.0.2.1 should not be assigned to any client or network device.
## Feature History and Information for SISF-Based Device Tracking

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>Support for policy priority was introduced. Priority is determined by how the policy is created. A manually created policy has the highest priority. This enables you to apply policy settings that are different from policies that are generated programmatically. More device tracking client features were introduced. The programmatic policy differs depending on the device tracking client feature that enables SISF-based device tracking.</td>
</tr>
</tbody>
</table>
CHAPTER 23

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.

- Information About 802.1x Port-Based Authentication, on page 405
- How to Configure 802.1x Port-Based Authentication, on page 436
- Monitoring 802.1x Statistics and Status, on page 484
- Feature Information for IEEE 802.1x Port-Based Authentication, on page 484

Information About 802.1x Port-Based Authentication

The 802.1x standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Note

TACACS is not supported with 802.1x authentication.

Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

<table>
<thead>
<tr>
<th>Client session</th>
<th>Maximum sessions supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum dot1x or MAB client sessions</td>
<td>2000</td>
</tr>
<tr>
<td>Maximum web-based authentication sessions</td>
<td>2000</td>
</tr>
<tr>
<td>Maximum dot1x sessions with critical-auth VLAN enabled and server re-initialized</td>
<td>2000</td>
</tr>
<tr>
<td>Maximum MAB sessions with various session features applied</td>
<td>2000</td>
</tr>
</tbody>
</table>
Port-Based Authentication Process

To configure IEEE 802.1X port-based authentication, you must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.

The AAA process begins with authentication. When 802.1x port-based authentication is enabled and the client supports 802.1x-compliant client software, these events occur:

- If the client identity is valid and the 802.1x authentication succeeds, the switch grants the client access to the network.

- If 802.1x authentication times out while waiting for an EAPOL message exchange and MAC authentication bypass is enabled, the switch can use the client MAC address for authorization. If the client MAC address is valid and the authorization succeeds, the switch grants the client access to the network. If the client MAC address is invalid and the authorization fails, the switch assigns the client to a guest VLAN that provides limited services if a guest VLAN is configured.

- If the switch gets an invalid identity from an 802.1x-capable client and a restricted VLAN is specified, the switch can assign the client to a restricted VLAN that provides limited services.

- If the RADIUS authentication server is unavailable (down) and inaccessible authentication bypass is enabled, the switch grants the client access to the network by putting the port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN.

Note: Inaccessible authentication bypass is also referred to as critical authentication or the AAA 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.
The switch re-authenticates a client when one of these situations occurs:

- Periodic re-authentication is enabled, and the re-authentication timer expires.

You can configure the re-authentication timer to use a switch-specific value or to be based on values from the RADIUS server.

After 802.1x authentication using a RADIUS server is configured, the switch uses timers based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute[29]).

The Session-Timeout RADIUS attribute (Attribute[27]) specifies the time after which re-authentication occurs.

The Termination-Action RADIUS attribute (Attribute[29]) specifies the action to take during re-authentication. The actions are Initialize and ReAuthenticate. When the Initialize action is set (the attribute value is DEFAULT), the 802.1x session ends, and connectivity is lost during re-authentication. When the ReAuthenticate action is set (the attribute value is RADIUS-Request), the session is not affected during re-authentication.

- You manually re-authenticate the client by entering the **dot1x re-authenticate interface interface-id** privileged EXEC command.
Port-Based Authentication Initiation and Message Exchange

During 802.1x authentication, the switch or the client can initiate authentication. If you enable authentication on a port by using the `authentication port-control auto` interface configuration command, the switch initiates authentication when the link state changes from down to up or periodically as long as the port remains up and unauthenticated. The switch sends an EAP-request/identity frame to the client to request its identity. Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client’s identity.

---

**Note**

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

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized. If the authentication fails, authentication can be retried, the port might be assigned to a VLAN that provides limited services, or network access is not granted.

The specific exchange of EAP frames depends on the authentication method being used.

**Figure 27: Message Exchange**

This figure shows a message exchange initiated by the client when the client uses the One-Time-Password (OTP) authentication method with a RADIUS server.

If 802.1x authentication times out while waiting for an EAPOL message exchange and MAC authentication bypass is enabled, the switch can authorize the client when the switch detects an Ethernet packet from the
client. The switch uses the MAC address of the client as its identity and includes this information in the RADIUS-access/request frame that is sent to the RADIUS server. After the server sends the switch the RADIUS-access/accept frame (authorization is successful), the port becomes authorized. If authorization fails and a guest VLAN is specified, the switch assigns the port to the guest VLAN. If the switch detects an EAPOL packet while waiting for an Ethernet packet, the switch stops the MAC authentication bypass process and starts 802.1x authentication.

**Figure 28: Message Exchange During MAC Authentication Bypass**

This figure shows the message exchange during MAC authentication bypass.

---

**Authentication Manager for Port-Based Authentication**

**Port-Based Authentication Methods**

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Mode</th>
<th>Single host</th>
<th>Multiple host</th>
<th>MDA</th>
<th>Multiple Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x</td>
<td></td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Per-user ACL</td>
<td></td>
<td>Per-user ACL</td>
<td>Per-user ACL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Filter-ID attribute</td>
<td></td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloadable ACL</td>
<td></td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Redirect URL</td>
<td></td>
<td>Redirect URL</td>
<td>Redirect URL</td>
</tr>
</tbody>
</table>
### Per-User ACLs and Filter-Ids

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Mode</th>
<th>Single host</th>
<th>Multiple host</th>
<th>MDA</th>
<th>Multiple Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC authentication bypass</td>
<td>VLAN assignment Per-user ACL Filter-ID attribute Downloadable ACL Redirect URL</td>
<td>VLAN assignment Per-user ACL Filter-ID attribute Downloadable ACL Redirect URL</td>
<td>VLAN assignment Per-user ACL Filter-ID attribute Downloadable ACL Redirect URL</td>
<td>VLAN assignment Per-user ACL Filter-ID attribute Downloadable ACL Redirect URL</td>
<td></td>
</tr>
<tr>
<td>Standalone web authentication</td>
<td>Proxy ACL, Filter-Id attribute, downloadable ACL</td>
<td>Proxy ACL, Filter-Id attribute, downloadable ACL</td>
<td>Proxy ACL, Filter-Id attribute, downloadable ACL</td>
<td>Proxy ACL, Filter-Id attribute, downloadable ACL</td>
<td></td>
</tr>
<tr>
<td>NAC Layer 2 IP validation</td>
<td>Filter-Id attribute Downloadable ACL Redirect URL</td>
<td>Filter-Id attribute Downloadable ACL Redirect URL</td>
<td>Filter-Id attribute Downloadable ACL Redirect URL</td>
<td>Filter-Id attribute Downloadable ACL Redirect URL</td>
<td></td>
</tr>
<tr>
<td>Web authentication as fallback method</td>
<td>Proxy ACL Filter-Id attribute Downloadable ACL</td>
<td>Proxy ACL Filter-Id attribute Downloadable ACL</td>
<td>Proxy ACL Filter-Id attribute Downloadable ACL</td>
<td>Proxy ACL Filter-Id attribute Downloadable ACL</td>
<td></td>
</tr>
</tbody>
</table>

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`.)

#### Note

Using role-based ACLs as Filter-Id is not recommended.

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 multi-auth ports. The ACL policy applied for one host does not effect the traffic of another host. If only one host is authenticated on a multi-host port, and the other hosts gain network access without authentication, the ACL policy for the first host can be applied to the other connected hosts by specifying any in the source address.
Port-Based Authentication Manager CLI Commands

The authentication-manager interface-configuration commands control all the authentication methods, such as 802.1x, MAC authentication bypass, and web authentication. The authentication manager commands determine the priority and order of authentication methods applied to a connected host.

The authentication manager commands control generic authentication features, such as host-mode, violation mode, and the authentication timer. Generic authentication commands include the authentication host-mode, authentication violation, and authentication timer interface configuration commands.

802.1x-specific commands begin with the dot1x keyword. For example, the authentication port-control auto interface configuration command enables authentication on an interface.

To disable dot1x on a switch, remove the configuration globally by using the no dot1x system-auth-control, and also remove it from all configured interfaces.

---

**Note**

If 802.1x authentication is globally disabled, other authentication methods are still enabled on that port, such as web authentication.

The authentication manager commands provide the same functionality as earlier 802.1x commands.

When filtering out verbose system messages generated by the authentication manager, the filtered content typically relates to authentication success. You can also filter verbose messages for 802.1x authentication and MAB authentication. There is a separate command for each authentication method:

- The no authentication logging verbose global configuration command filters verbose messages from the authentication manager.
- The no dot1x logging verbose global configuration command filters 802.1x authentication verbose messages.
- The no mab logging verbose global configuration command filters MAC authentication bypass (MAB) verbose messages.

<table>
<thead>
<tr>
<th>The authentication manager commands in Cisco IOS Release 12.2(50)SE or later</th>
<th>The equivalent 802.1x commands in Cisco IOS Release 12.2(46)SE and earlier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication control-direction {both</td>
<td>in}</td>
<td>dot1x control-direction {both</td>
</tr>
<tr>
<td>authentication event</td>
<td>dot1x auth-fail vlan</td>
<td>Enable the restricted VLAN on a port.</td>
</tr>
<tr>
<td></td>
<td>dot1x critical (interface configuration)</td>
<td>Enable the inaccessible-authentication-bypass feature.</td>
</tr>
<tr>
<td></td>
<td>dot1x guest-vlan6</td>
<td>Specify an active VLAN as an 802.1x guest VLAN.</td>
</tr>
</tbody>
</table>
The authentication manager commands in Cisco IOS Release 12.2(50)SE or later

<table>
<thead>
<tr>
<th>Description</th>
<th>The equivalent 802.1x commands in Cisco IOS Release 12.2(46)SE and earlier</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a port to use web authentication as a fallback method for clients that do not support 802.1x authentication.</td>
<td>authentication fallback fallback-profile</td>
<td>dot1x fallback fallback-profile</td>
</tr>
<tr>
<td>Allow a single host (client) or multiple hosts on an 802.1x-authorized port.</td>
<td>authentication host-mode [single-host</td>
<td>multi-host</td>
</tr>
<tr>
<td>Provides the flexibility to define the order of authentication methods to be used.</td>
<td>authentication order</td>
<td>mab</td>
</tr>
<tr>
<td>Enable periodic re-authentication of the client.</td>
<td>authentication periodic</td>
<td>dot1x reauthentication</td>
</tr>
<tr>
<td>Enable manual control of the authorization state of the port.</td>
<td>authentication port-control [auto</td>
<td>force-authorized</td>
</tr>
<tr>
<td>Set the 802.1x timers.</td>
<td>authentication timer</td>
<td>dot1x timeout</td>
</tr>
<tr>
<td>Configure the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.</td>
<td>authentication violation [protect</td>
<td>restrict</td>
</tr>
</tbody>
</table>

### Ports in Authorized and Unauthorized States

During 802.1x authentication, depending on the switch port state, the switch can grant a client access to the network. The port starts in the unauthorized state. While in this state, the port that is not configured as a voice VLAN port disallows all ingress and egress traffic except for 802.1x authentication, CDP, and STP packets. When a client is successfully authenticated, the port changes to the authorized state, allowing all traffic for the client to flow normally. If the port is configured as a voice VLAN port, the port allows VoIP traffic and 802.1x protocol packets before the client is successfully authenticated.

**Note**

CDP bypass is not supported and may cause a port to go into err-disabled state.

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.

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 and voice VLAN. Each host is individually authenticated. There is no limit to the number of data or voice device that can be authenticated on a multiauth port.

---

**Note**

When a port is in multiple-authentication mode, 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.
- After a VLAN is assigned to a host on the port, subsequent hosts must have matching VLAN information or be denied access to the port.
- You cannot configure a guest VLAN or an auth-fail VLAN in multi-auth mode.
- The behavior of the critical-auth VLAN is not changed for multi-auth mode. When a host tries to authenticate and the server is not reachable, all authorized hosts are reinitialized in the configured VLAN.
Multi-auth Per User VLAN assignment

The Multi-auth Per User VLAN assignment feature allows you to create multiple operational access VLANs based on VLANs assigned to the clients on the port that has a single configured access VLAN. The port configured as an access port where the traffic for all the VLANs associated with data domain is not dot1q tagged, and these VLANs are treated as native VLANs.

The number of hosts per multi-auth port is 8, however there can be more hosts.

The 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 assigns incorrect IPv6 address to itself. Such a host is unable to get access to the network.

  The workaround is to enable the IPv6 first hop security so that the broadcast ICMPv6 packets are converted to unicast and sent out from multi-auth enabled ports. The packet is replicated for each client in multi-auth port belonging to the VLAN and the destination MAC is set to an individual client. Ports having one VLAN, ICMPv6 packets broadcast normally.

• **IP multicast**: Multicast traffic destined to a multicast group gets replicated for different VLANs if the hosts on those VLANs join the multicast group. When two hosts in different VLANs join a multicast group (on the same multi-auth port), two copies of each multicast packet are sent out from that port.

### MAC Move

When a MAC address is authenticated on one switch port, that address is not allowed on another authentication manager-enabled port of the switch. If the switch detects that same MAC address on another authentication manager-enabled port, the address is not allowed.

There are situations where a MAC address might need to move from one port to another on the same switch. For example, when there is another device (for example a hub or an IP phone) between an authenticated host and a switch port, you might want to disconnect the host from the device and connect it directly to another port on the same switch.

You can globally enable MAC move so the device is reauthenticated on the new port. When a host moves to a second port, the session on the first port is deleted, and the host is reauthenticated on the new port. MAC move is supported on all host modes. (The authenticated host can move to any port on the switch, no matter which host mode is enabled on 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.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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

Note

To view debug logs for RADIUS and AAA, use the show platform software trace message smd command. For more information, see the Tracing Commands section in Command Reference Guide.
This table lists the AV pairs and when they are sent by the switch.

Table 61: Accounting AV Pairs

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>AV Pair Name</th>
<th>START</th>
<th>INTERIM</th>
<th>STOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute[1]</td>
<td>User-Name</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[4]</td>
<td>NAS-IP-Address</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[5]</td>
<td>NAS-Port</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[8]</td>
<td>Framed-IP-Address</td>
<td>Never</td>
<td>Sometimes¹¹</td>
<td>Sometimes</td>
</tr>
<tr>
<td>Attribute[30]</td>
<td>Called-Station-ID</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[31]</td>
<td>Calling-Station-ID</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[40]</td>
<td>Acct-Status-Type</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[41]</td>
<td>Acct-Delay-Time</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[42]</td>
<td>Acct-Input-Octets</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[43]</td>
<td>Acct-Output-Octets</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[47]</td>
<td>Acct-Input-Packets</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[48]</td>
<td>Acct-Output-Packets</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[44]</td>
<td>Acct-Session-ID</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[45]</td>
<td>Acct-Authentic</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[46]</td>
<td>Acct-Session-Time</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[49]</td>
<td>Acct-Terminate-Cause</td>
<td>Never</td>
<td>Never</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[61]</td>
<td>NAS-Port-Type</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
</tbody>
</table>

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

802.1x Readiness Check

The 802.1x readiness check monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable. You use an alternate authentication such as MAC authentication bypass or web authentication for the devices that do not support 802.1x functionality.

This feature only works if the supplicant on the client supports a query with the NOTIFY EAP notification packet. The client must respond within the 802.1x timeout value.
Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by their hostname or IP address, hostname and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as the fail-over backup to the first one. The RADIUS host entries are tried in the order that they were configured.

802.1x Authentication with VLAN Assignment

The switch supports 802.1x authentication with VLAN assignment. After successful 802.1x authentication of a port, the RADIUS server sends the VLAN assignment to configure the switch port. The RADIUS server 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.

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. The user is marked unauthorized if the Filter-Id sent from the RADIUS server is not configured on the device. Because of limited support of Cisco IOS access lists on the switch, the Filter-Id attribute is supported only for IP ACLs numbered in the range of 1 to 199 (IP standard ACLs) and 1300 to 2699 (IP extended ACLs).

The maximum size of the per-user ACL is 4000 ASCII characters but is limited by the maximum size of RADIUS-server per-user ACLs.

You must meet the following prerequisites to configure per-user ACLs:

- Enable AAA authentication.
- Enable AAA authorization by using the network keyword to allow interface configuration from the RADIUS server.
- Enable 802.1x authentication.
- Configure the user profile and VSAs on the RADIUS server.
- Configure the 802.1x port for single-host mode.

Note

Per-user ACLs are supported only in single-host mode.

802.1x Authentication with Downloadable ACLs and Redirect URLs

You can download ACLs and redirect URLs from a RADIUS server to the switch during 802.1x authentication or MAC authentication bypass of the host. You can also download ACLs during web authentication.

Note

A downloadable ACL is also referred to as a dACL.
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.

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 bypass in the single host mode. You must configure a static ACL on the interface to support Cisco Discovery Protocol 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.

---

**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.

**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.
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.

You can configure a VLAN to be both the guest VLAN and the restricted VLAN if you want to provide the same services to both types of users.

Without this feature, the client attempts and fails authentication indefinitely, and the switch port remains in the spanning-tree blocking state. With this feature, you can configure the switch port to be in the restricted VLAN after a specified number of authentication attempts (the default value is 3 attempts).

The authenticator counts the failed authentication attempts for the client. When this count exceeds the configured maximum number of authentication attempts, the port moves to the restricted VLAN. The failed attempt count increments when the RADIUS server replies with either an EAP failure or an empty response without an EAP packet. When the port moves into the restricted VLAN, the failed attempt counter resets.

Users who fail authentication remain in the restricted VLAN until the next re-authentication attempt. A port in the restricted VLAN tries to re-authenticate at configured intervals (the default is 60 seconds). If re-authentication fails, the port remains in the restricted VLAN. If re-authentication is successful, the port moves either to the configured VLAN or to a VLAN sent by the RADIUS server. You can disable re-authentication. If you do this, the only way to restart the authentication process is for the port to receive a link down or EAP logoff event. We recommend that you keep re-authentication enabled if a client might...
connect through a hub. When a client disconnects from the hub, the port might not receive the *link down* or *EAP logoff* event.

After a port moves to the restricted VLAN, a simulated EAP success message is sent to the client. This prevents clients from indefinitely attempting authentication. Some clients (for example, devices running Windows XP) cannot implement DHCP without EAP success.

Restricted VLANs are supported on 802.1x ports in all host modes and on Layer 2 ports.

You can configure any active VLAN except an RSPAN VLAN, a primary private VLAN, or a voice VLAN as an 802.1x restricted VLAN. The restricted VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

Other security port features such as dynamic ARP Inspection, DHCP snooping, and IP source guard can be configured independently on a restricted VLAN.

### 802.1x Authentication with Inaccessible Authentication Bypass

Use the inaccessible authentication bypass feature, also referred to as *critical authentication* or the *AAA fail policy*, when the switch cannot reach the configured RADIUS servers and new hosts cannot be authenticated. You can configure the switch to connect those hosts to *critical ports*.

When a new host tries to connect to the critical port, that host is moved to a user-specified access VLAN, the *critical VLAN*. The administrator gives limited authentication to the hosts.

When the switch tries to authenticate a host connected to a critical port, the switch checks the status of the configured RADIUS server. If a server is available, the switch can authenticate the host. However, if all the RADIUS servers are unavailable, the switch grants network access to the host and puts the port in the *critical-authentication* state, which is a special case of the authentication state.

---

**Note**

If *critical authentication* is configured on interface, then vlan used for critical authorization (*critical vlan*) should be active on the switch. If the *critical vlan* is inactive (or) down, *critical authentication* session will keep trying to enable inactive vlan and fail repeatedly. This can lead to large amount of memory holding.

### Inaccessible Authentication Bypass Support on Multiple-Authentication Ports

When a port is configured on any host mode and the AAA server is unavailable, the port is then configured to multi-host mode and moved to the critical VLAN. To support this inaccessible bypass on multiple-authentication (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.
In inaccessible authentication bypass, 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**

In inaccessible authentication bypass interacts with these features:

- Guest VLAN—Inaccessible authentication bypass is compatible with guest VLAN. When a guest VLAN is enabled on 802.1x 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.

**802.1x Critical Voice VLAN**

When an IP phone connected to a port is authenticated by the Cisco Identity Services Engine (ISE), the phone is put into the voice domain. If the ISE 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.

**Note**
Dynamic assignment of critical voice VLAN is not supported with nested service templates. It causes the device to switch between VLANs continuously in a loop.

You can enter the `authentication event server dead action authorize voice interface configuration` command to configure the critical voice VLAN feature. When the ISE 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 Cisco Discovery Protocol (Cisco devices) or through LLDP or DHCP.

You can configure the voice VLAN for a port by entering the `switchport voice vlan vlan-id interface configuration` command.

This feature is supported in multidomain and multi-auth host modes. Although you can enter the command when the switch in single-host or multi-host mode, the command has no effect unless the device changes to multidomain or multi-auth host mode.

### 802.1x User Distribution

You can configure 802.1x user distribution to load-balance users with the same group name across multiple different VLANs.

The VLANs are either supplied by the RADIUS server or configured through the switch CLI under a VLAN group name.

- Configure the RADIUS server to send more than one VLAN name for a user. The multiple VLAN names can be sent as part of the response to the user. The 802.1x user distribution tracks all the users in a particular VLAN and achieves load balancing by moving the authorized user to the least populated VLAN.

- Configure the RADIUS server to send a VLAN group name for a user. The VLAN group name can be sent as part of the response to the user. You can search for the selected VLAN group name among the VLAN group names that you configured by using the switch CLI. If the VLAN group name is found, the corresponding VLANs under this VLAN group name are searched to find the least populated VLAN. Load balancing is achieved by moving the corresponding authorized user to that VLAN.

**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

- Private VLAN—You can assign a client to a private VLAN.

- Network Edge Access Topology (NEAT)—MAB and NEAT are mutually exclusive. You cannot enable MAB when NEAT is enabled on an interface, and you should not enable NEAT when MAB is enabled on an interface.

Cisco IOS Release 12.2(55)SE and later supports filtering of verbose MAB system messages

**Network Admission Control Layer 2 IEEE 802.1x Validation**

The switch supports the Network Admission Control (NAC) Layer 2 IEEE 802.1x validation, which checks the antivirus condition or posture of endpoint systems or clients before granting the devices network access. With NAC Layer 2 IEEE 802.1x validation, you can do these tasks:

- Download the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute[29]) from the authentication server.

- Set the number of seconds between re-authentication attempts as the value of the Session-Timeout RADIUS attribute (Attribute[27]) and get an access policy against the client from the RADIUS server.

- Set the action to be taken when the switch tries to re-authenticate the client by using the Termination-Action RADIUS attribute (Attribute[29]). If the value is the DEFAULT or is not set, the session ends. If the value is RADIUS-Request, the re-authentication process starts.

- Set the list of VLAN number or name or VLAN group name as the value of the Tunnel Group Private ID (Attribute[81]) and the preference for the VLAN number or name or VLAN group name as the value
of the Tunnel Preference (Attribute[83]). If you do not configure the Tunnel Preference, the first Tunnel Group Private ID (Attribute[81]) attribute is picked up from the list.

- View the NAC posture token, which shows the posture of the client, by using the `show authentication` privileged EXEC command.

- Configure secondary private VLANs as guest VLANs.

Configuring NAC Layer 2 IEEE 802.1x validation is similar to configuring IEEE 802.1x port-based authentication except that you must configure a posture token on the RADIUS server.

### Flexible Authentication Ordering

You can use flexible authentication ordering to configure the order of methods that a port uses to authenticate a new host. The IEEE 802.1X Flexible Authentication feature supports three authentication methods:

- **dot1X**—IEEE 802.1X authentication is a Layer 2 authentication method.
- **mab**—MAC-Authentication Bypass is a Layer 2 authentication method.
- **webauth**—Web authentication is a Layer 3 authentication method.

Using this feature, you can control which ports use which authentication methods, and you can control the failover sequencing of methods on those ports. For example, MAC authentication bypass and 802.1x can be the primary or secondary authentication methods, and web authentication can be the fallback method if either or both of those authentication attempts fail.

The IEEE 802.1X Flexible Authentication feature supports the following host modes:

- **multi-auth**—Multiauthentication allows one authentication on a voice VLAN and multiple authentications on the data VLAN.
- **multi-domain**—Multidomain authentication allows two authentications: one on the voice VLAN and one on the data VLAN.

### Open1x Authentication

Open1x authentication allows a device access to a port before that device is authenticated. When open authentication is configured, a new host can pass traffic according to the access control list (ACL) defined on the port. After the host is authenticated, the policies configured on the RADIUS server are applied to that host.

You can configure open authentication with these scenarios:

- **Single-host mode with open authentication**—Only one user is allowed network access before and after authentication.
- **MDA mode with open authentication**—Only one user in the voice domain and one user in the data domain are allowed.
- **Multiple-hosts mode with open authentication**—Any host can access the network.
- **Multiple-authentication mode with open authentication**—Similar to MDA, except multiple hosts can be authenticated.
If open authentication is configured, it takes precedence over other authentication controls. This means that if you use the `authentication open` interface configuration command, the port will grant access to the host irrespective of the `authentication port-control` interface configuration command.

### Multidomain Authentication

The switch supports multidomain authentication (MDA), which allows both a data device and voice device, such as an IP phone (Cisco or non-Cisco), to authenticate on the same switch port. The port is divided into a data domain and a voice domain.

For all host modes, the line protocol stays up before authorization when port-based authentication is configured.

MDA does not enforce the order of device authentication. However, for best results, we recommend that a voice device is authenticated before a data device on an MDA-enabled port.

Follow these guidelines for configuring MDA:

- You must configure a switch port for MDA.
- You must configure the voice VLAN for the IP phone when the host mode is set to multidomain.
- Voice VLAN assignment on an MDA-enabled port is supported Cisco IOS Release 12.2(40)SE and later.
- To authorize a voice device, the AAA server must be configured to send a Cisco Attribute-Value (AV) pair attribute with a value of `device-traffic-class=voice`. Without this value, the switch treats the voice device as a data device.
- The guest VLAN and restricted VLAN features only apply to the data devices on an MDA-enabled port. The switch treats a voice device that fails authorization as a data device.
- If more than one device attempts authorization on either the voice or the data domain of a port, it is error disabled.
- Until a device is authorized, the port drops its traffic. Non-Cisco IP phones or voice devices are allowed into both the data and voice VLANs. The data VLAN allows the voice device to contact a DHCP server to obtain an IP address and acquire the voice VLAN information. After the voice device starts sending on the voice VLAN, its access to the data VLAN is blocked.
- A voice device MAC address that is binding on the data VLAN is not counted towards the port security MAC address limit.
- MDA can use MAC authentication bypass as a fallback mechanism to allow the switch port to connect to devices that do not support IEEE 802.1x authentication.
- When a `data` or a `voice` device is detected on a port, its MAC address is blocked until authorization succeeds. If the authorization fails, the MAC address remains blocked for 5 minutes.
- If more than five devices are detected on the `data` VLAN or more than one voice device is detected on the `voice` VLAN while a port is unauthorized, the port is error disabled.
• When a port host mode is changed from single- or multihost to multidomain mode, an authorized data device remains authorized on the port. However, a Cisco IP phone that has been allowed on the port voice VLAN is automatically removed and must be reauthenticated on that port.

• Active fallback mechanisms such as guest VLAN and restricted VLAN remain configured after a port changes from single- or multihost mode to multidomain mode.

• Switching a port host mode from multidomain to single- or multihost mode removes all authorized devices from the port.

• If a data domain is authorized first and placed in the guest VLAN, non-IEEE 802.1x-capable voice devices need to tag their packets on the voice VLAN to trigger authentication.

• We do not recommend per-user ACLs with an MDA-enabled port. An authorized device with a per-user ACL policy might impact traffic on both the voice and data VLANs of the port. If used, only one device on the port should enforce per-user ACLs.

802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT)

The Network Edge Access Topology (NEAT) feature extends identity to areas outside the wiring closet (such as conference rooms). This allows any type of device to authenticate on the port.

• 802.1x switch supplicant: You can configure a switch to act as a supplicant to another switch by using the 802.1x supplicant feature. This configuration is helpful in a scenario, where, for example, a switch is outside a wiring closet and is connected to an upstream switch through a trunk port. A switch configured with the 802.1x switch supplicant feature authenticates with the upstream switch for secure connectivity. Once the supplicant switch authenticates successfully the port mode changes from access to trunk in an authenticator switch. In a supplicant switch you must manually configure trunk when enabling CISP.

• If the access VLAN is configured on the authenticator switch, it becomes the native VLAN for the trunk port after successful authentication.

In the default state, when you connect a supplicant switch to an authenticator switch that has BPDU guard enabled, the authenticator port could be error-disabled if it receives a Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets before the supplicant switch has authenticated. Beginning with Cisco IOS Release 15.0(1)SE, you can control traffic exiting the supplicant port during the authentication period. Entering the `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.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you globally enable BPDU guard on the authenticator switch by using the <code>spanning-tree portfast bpduguard default</code> global configuration command, entering the <code>dot1x supplicant controlled transient</code> command does not prevent the BPDU violation.</td>
</tr>
</tbody>
</table>
You can enable MDA or multiauth mode on the authenticator switch interface that connects to one more supplicant switches. Multihost mode is not supported on the authenticator switch interface.

When you reboot an authenticator switch with single-host mode enabled on the interface, the interface may move to err-disabled state before authentication. To recover from err-disabled state, flap the authenticator port to activate the interface again and initiate authentication.

Use the `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 ISE. (You can configure this under the `group` or the `user` settings.)

*Figure 29: Authenticator and Supplicant Switch using CISP*

<table>
<thead>
<tr>
<th></th>
<th>Workstations (clients)</th>
<th></th>
<th>Supplicant switch (outside wiring closet)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Authenticator switch</td>
<td>4</td>
<td>Cisco ISE</td>
</tr>
<tr>
<td>5</td>
<td>Trunk port</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*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.

**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 16000005000000B288508E5:

```
Device# show authentication sessions
Interface   MAC Address   Method   Domain   Status   Session ID
Fa4/0/4     0000.0000.0203  mab     DATA     Authz Success 16000005000000B288508E5
```

This is an example of how the session ID appears in the syslog output. The session ID in this example is also 16000005000000B288508E5:

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 16000005000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 16000005000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client (0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 16000005000000B288508E5
```

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 62: Default 802.1x Authentication Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 802.1x enable state</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Per-port 802.1x enable state</td>
<td>Disabled (force-authorized). The port sends and receives normal traffic without 802.1x-based authentication of the client.</td>
</tr>
<tr>
<td>AAA</td>
<td>Disabled.</td>
</tr>
<tr>
<td>RADIUS server</td>
<td>• None specified. • 1645. • 1646. • None specified.</td>
</tr>
<tr>
<td>Host mode</td>
<td>Single-host mode.</td>
</tr>
<tr>
<td>Control direction</td>
<td>Bidirectional control.</td>
</tr>
<tr>
<td>Periodic re-authentication</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Number of seconds between re-authentication attempts</td>
<td>3600 seconds.</td>
</tr>
<tr>
<td>Re-authentication number</td>
<td>2 times (number of times that the switch restarts the authentication process before the port changes to the unauthorized state).</td>
</tr>
<tr>
<td>Quiet period</td>
<td>60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client).</td>
</tr>
<tr>
<td>Retransmission time</td>
<td>30 seconds (number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before resending the request).</td>
</tr>
<tr>
<td>Maximum retransmission number</td>
<td>2 times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process).</td>
</tr>
</tbody>
</table>
### Default Setting

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client timeout period</td>
<td>30 seconds (when relaying a request from the authentication server to the client, the amount of time the switch waits for a response before resending the request to the client.)</td>
</tr>
<tr>
<td>Authentication server timeout period</td>
<td>30 seconds (when relaying a response from the client to the authentication server, the amount of time the switch waits for a reply before resending the response to the server.) You can change this timeout period by using the dot1x timeout server-timeout interface configuration command.</td>
</tr>
<tr>
<td>Inactivity timeout</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Guest VLAN</td>
<td>None specified.</td>
</tr>
<tr>
<td>Inaccessible authentication bypass</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Restricted VLAN</td>
<td>None specified.</td>
</tr>
<tr>
<td>Authenticator (switch) mode</td>
<td>None specified.</td>
</tr>
<tr>
<td>MAC authentication bypass</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Voice-aware security</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>

### 802.1x Authentication Configuration Guidelines

#### 802.1x Authentication

These are the 802.1x authentication configuration guidelines:

- You must enable SISF-Based device tracking to use 802.1x authentication. By default, SISF-Based device tracking is disabled on a switch.
- When 802.1x authentication is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.
- If the VLAN to which an 802.1x-enabled port is assigned changes, this change is transparent and does not affect the switch. For example, this change occurs if a port is assigned to a RADIUS server-assigned VLAN and is then assigned to a different VLAN after re-authentication.

If the VLAN to which an 802.1x port is assigned to shut down, disabled, or removed, the port becomes unauthorized. For example, the port is unauthorized after the access VLAN to which a port is assigned shuts down or is removed.

- The 802.1x protocol is supported on Layer 2 static-access ports, voice VLAN ports, and Layer 3 routed ports, but it is not supported on these port types:
  - **Dynamic ports**—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1x authentication on a dynamic port, an error message appears, and 802.1x...
authentication is not enabled. If you try to change the mode of an 802.1x-enabled port to dynamic, an error message appears, and the port mode is not changed.

- EtherChannel port—Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an 802.1x port. If you try to enable 802.1x authentication on an EtherChannel port, an error message appears, and 802.1x authentication is not enabled.

- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable 802.1x authentication on a port that is a SPAN or RSPAN destination port. However, 802.1x authentication is disabled until the port is removed as a SPAN or RSPAN destination port. You can enable 802.1x authentication on a SPAN or RSPAN source port.

- Before globally enabling 802.1x authentication on a switch by entering the `dot1x system-auth-control` global configuration command, remove the EtherChannel configuration from the interfaces on which 802.1x authentication and EtherChannel are configured.

- Cisco IOS Release 12.2(55)SE and later supports filtering of system messages related to 802.1x authentication.

### VLAN Assignment, Guest VLAN, Restricted VLAN, and Inaccessible Authentication Bypass

These are the configuration guidelines for VLAN assignment, guest VLAN, restricted VLAN, and inaccessible authentication bypass:

- When 802.1x authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.

- 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.
• If the CTS links are in Critical Authentication mode and the master reloads, the policy where SGT was configured on a device will not be available on the new master. This is because the internal bindings will not be synced to the standby switch in a 3750-X switch stack.

• You can configure any VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN. The restricted VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

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.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dot1x test eapol-capable [interface interface-id]</td>
<td>Enables the 802.1x readiness check on the switch.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# dot1x test eapol-capable interface gigabitethernet1/0/13 DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-e1-e2-4f-1e-a3 is EAPOL capable</td>
<td>(Optional) For interface-id specify the port on which to check for IEEE 802.1x readiness.</td>
</tr>
<tr>
<td><strong>Note</strong> If you omit the optional interface keyword, all interfaces on the switch are tested.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> dot1x test timeout timeout</td>
<td>(Optional) Configures the timeout used to wait for EAPOL response. The range is from 1 to 65535 seconds. The default is 10 seconds.</td>
</tr>
</tbody>
</table>
### Configuring Voice Aware 802.1x Security

To use voice aware IEEE 802.1x authentication, the switch must be running the LAN base image.

You use the voice aware 802.1x security feature 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 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td><code>end</code> <strong>Example:</strong> Device(config)# <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>show running-config</code> <strong>Example:</strong> Device# <code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>copy running-config startup-config</code> <strong>Example:</strong> Device# <code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> errdisable detect cause security-violation shutdown vlan</td>
<td>Shut down any VLAN on which a security violation error occurs.</td>
</tr>
<tr>
<td><strong>Note</strong> If the <strong>shutdown vlan</strong> keywords are not included, the entire port enters the error-disabled state and shuts down.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> errdisable recovery cause security-violation</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> clear errdisable interface interface-id vlan [vlan-list]</td>
<td>(Optional) Reenable individual VLANs that have been error disabled.</td>
</tr>
<tr>
<td></td>
<td>• For interface-id specify the port on which to reenable individual VLANs.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For vlan-list specify a list of VLANs to be re-enabled. If vlan-list is not specified, all VLANs are re-enabled.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Enter the following:</td>
<td>(Optional) Re-enable an error-disabled VLAN, and clear all error-disable indications.</td>
</tr>
<tr>
<td>• shutdown</td>
<td></td>
</tr>
<tr>
<td>• no shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> show errdisable detect</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

### Example

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 gigabitethernet40/2 vlan
```

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

### 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
Configuring IEEE 802.1x Port-Based Authentication

- the maximum number of allowed about devices have been authenticated on the port

Beginning in privileged EXEC mode, follow these steps to configure the security violation actions on the switch:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>aaa new-model</code></td>
<td>Enables AAA.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# aaa new-model</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>aaa authentication dot1x {default} method1</code></td>
<td>Creates an 802.1x authentication method list.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# aaa authentication dot1x default group radius</code></td>
<td>To create a default list that is used when a named list is <em>not</em> specified in the <code>authentication</code> command, use the <code>default</code> keyword followed by the method that is to be used in default situations. The default method list is automatically applied to all ports. For <code>method1</code>, enter the <code>group radius</code> keywords to use the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>interface interface-id</code></td>
<td>Specifies the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# interface gigabitethernet1/0/4</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>switchport mode access</code></td>
<td>Sets the port to access mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-if)# switchport mode access</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>`authentication violation {shutdown</td>
<td>restrict</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-if)# authentication</code></td>
<td></td>
</tr>
</tbody>
</table>

Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| violation restrict | - protect: Drop packets from any new device that sends traffic to the port.  
- replace: Removes the current session and authenticates with the new host. |

### Example:

```bash
Device(config-if)# end
```

## 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.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A user connects to a port on the switch.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Authentication is performed.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>The switch sends a start message to an accounting server.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Re-authentication is performed, as necessary.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>The switch sends an interim accounting update to the accounting server that is based on the result of re-authentication.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>The user disconnects from the port.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>The switch sends a stop message to the accounting server.</td>
<td></td>
</tr>
</tbody>
</table>
# Configuring 802.1x Port-Based Authentication

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

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>aaa new-model</code></td>
<td>Enables AAA.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# aaa new-model</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>aaa authentication dot1x {default} method1</code></td>
<td>Creates an 802.1x authentication method list.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>To create a default list that is used when a named list is not specified in the <code>authentication</code> command, use the <code>default</code> keyword followed by the method that is to be used in default situations. The default method list is automatically applied to all ports. For <code>method1</code>, enter the <code>group radius</code> keywords to use the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# aaa authentication dot1x default group radius</code></td>
<td>Note: Though other keywords are visible in the command-line help string, only the <code>group radius</code> keywords are supported.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>dot1x system-auth-control</code></td>
<td>Enables 802.1x authentication globally on the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# dot1x system-auth-control</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>aaa authorization network {default} group radius</code></td>
<td>(Optional) Configures the switch to use user-RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# aaa authorization network default group radius</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring IEEE 802.1x Port-Based Authentication

<table>
<thead>
<tr>
<th>Step 6</th>
<th><strong>radius server server name</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Optional) Specifies the IP address of the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# radius server rsim address ipv4 124.2.2.12</td>
<td></td>
</tr>
</tbody>
</table>

| Step 7 | **address {ipv4 | ipv6} ip address** | **Purpose** |
|--------|---------------------------------|-------------|
|        | Configures the IP address for the RADIUS server. |
| Example: | Device(config-radius-server)# address ipv4 10.0.1.12 |

<table>
<thead>
<tr>
<th>Step 8</th>
<th><strong>key string</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-radius-server)# key rad123</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th><strong>exit</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exits the RADIUS server mode and enters the global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-radius-server)# exit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th><strong>interface interface-id</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specifies the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# interface gigabitethernet1/0/2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th><strong>switchport mode access</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Optional) Sets the port to access mode only if you configured the RADIUS server in Step 6 and Step 7.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# switchport mode access</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 12</th>
<th><strong>authentication port-control auto</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enables 802.1x authentication on the port.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# authentication port-control auto</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring IEEE 802.1x Port-Based Authentication

#### Step 13

**Command or Action**: dot1x pae authenticator

**Example**:

```
Device(config-if)# dot1x pae authenticator
```

**Purpose**: Sets the interface Port Access Entity to act only as an authenticator and ignore messages meant for a supplicant.

#### Step 14

**Command or Action**: end

**Example**:

```
Device(config-if)# end
```

**Purpose**: Returns to privileged EXEC mode.

---

### Configuring Switch-to-RADIUS-Server Communication

Follow these steps to configure the RADIUS server parameters:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip radius source-interface</td>
<td>Specifies that the RADIUS packets have the IP address of the indicated interface.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip radius source-interface vlan 80</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> radius server <strong>server name</strong></td>
<td>(Optional) Specifies the IP address of the RADIUS server.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# radius server rsim address ipv4 124.2.2.12</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the Host Mode

Beginning in privileged EXEC mode, follow these steps to allow multiple hosts (clients) on an IEEE 802.1x-authorized port that has the authentication port-control interface configuration command set to auto. Use the multi-domain keyword to configure and enable multidomain authentication (MDA), which allows both a host and a voice device, such as an IP phone (Cisco or non-Cisco), on the same switch port. This procedure is optional.

**Procedure**

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

---

### Configuring IEEE 802.1x Port-Based Authentication

#### Purpose

**Command or Action**

**Step 5**

`address {ipv4 | ipv6} ip address`

Example:

```
Device(config-radius-server)# address ipv4 10.0.1.2 auth-port 1550 acct-port 1560
```

Purpose: Configures the IP address for the RADIUS server.

**Step 6**

`key string`

Example:

```
Device(config-radius-server)# key rad123
```

Purpose: (Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.

**Step 7**

`exit`

Example:

```
Device(config-radius-server)# exit
```

Purpose: Exits the RADIUS server mode and enters the global configuration mode.

**Step 8**

`radius-server dead-criteria tries num-tries`

Example:

```
Device(config)# radius-server
dead-criteria tries 30
```

Purpose: Specifies the number of unanswered sent messages to a RADIUS server before considering the server to be inactive. The range of `num-tries` is 1 to 100.

**Step 9**

`end`

Example:

```
Device(config)# end
```

Purpose: Returns to privileged EXEC mode.
### Configuring IEEE 802.1x Port-Based Authentication

#### Configuring the Host Mode

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# configure terminal</td>
<td>Specifies the port to which multiple hosts are indirectly attached, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Allows multiple hosts (clients) on an 802.1x-authorized port.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# interface gigabitethernet2/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> authentication host-mode [multi-auth</td>
<td>The keywords have these meanings:</td>
</tr>
<tr>
<td>multi-domain</td>
<td>• multi-auth—Allow multiple authenticated clients on both the voice VLAN and data VLAN.</td>
</tr>
<tr>
<td>multi-host</td>
<td>Note The multi-auth keyword is only available with the authentication host-mode command.</td>
</tr>
<tr>
<td>single-host</td>
<td>• multi-host—Allow multiple hosts on an 802.1x-authorized port after a single host has been authenticated.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# authentication host-mode multi-host</td>
<td>• 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.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Note You must configure the voice VLAN for the IP phone when the host mode is set to multi-domain.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Make sure that the authentication port-control interface configuration command is set to auto for the specified interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Configuring Periodic Re-Authentication

You can enable periodic 802.1x client re-authentication and specify how often it occurs. If you do not specify a time period before enabling re-authentication, the number of seconds between attempts is 3600.

Beginning in privileged EXEC mode, follow these steps to enable periodic re-authentication of the client and to configure the number of seconds between re-authentication attempts. This procedure is optional.

**Procedure**

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

**Example:**

```
Device# configure terminal
```

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><code>interface interface-id</code></td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Device(config)# interface gigabitethernet2/0/1
```

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><code>authentication periodic</code></td>
<td>Enables periodic re-authentication of the client, which is disabled by default.</td>
</tr>
</tbody>
</table>

**Example:**

```
Device(config-if)# authentication periodic
```

**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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>`authentication timer {inactivity</td>
<td>reauthenticate</td>
</tr>
</tbody>
</table>

**Example:**

```
Device(config-if)# authentication timer reauthenticate 180
```

The `authentication timer` keywords have these meanings:

- **inactivity**—Interval in seconds after which if there is no activity from the client then it is unauthorized
- **reauthenticate**—Time in seconds after which an automatic re-authentication attempt is initiated
- **restart value**—Interval in seconds after which an attempt is made to authenticate an unauthorized port
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• unauthorized value—Interval in seconds after which an unauthorized session will get deleted</td>
<td>This command affects the behavior of the switch only if periodic re-authentication is enabled.</td>
</tr>
</tbody>
</table>

### Example:

#### Step 5

```
Device(config-if)# end
```

### Changing the Quiet Period

When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. The `authentication timer restart` interface configuration command controls the idle period. A failed authentication of the client might occur because the client provided an invalid password. You can provide a faster response time to the user by entering a number smaller than the default.

Beginning in privileged EXEC mode, follow these steps to change the quiet period. This procedure is optional.

#### Procedure

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

  ```
  configure terminal
  ```

  **Example:**

  `Device# configure terminal`

| Step 2

  ```
  interface interface-id
  ```

  **Example:**

  `Device(config)# interface gigabitethernet2/0/1`

| Step 3

  ```
  authentication timer restart seconds
  ```

  **Example:**

  `Device(config-if)# authentication timer restart 30`

  **Note:**
  - 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:**

  `Device(config-if)# end`

  Returns to privileged EXEC mode.
### 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.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Device(config)# interface gigabitethernet2/0/1</td>
<td></td>
</tr>
</tbody>
</table>
### Setting the Switch-to-Client Frame-Retransmission Number

In addition to changing the switch-to-client retransmission time, you can change the number of times that the switch sends an EAP-request/identity frame (assuming no response is received) to the client before restarting the authentication process.

#### Note
You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to set the switch-to-client frame-retransmission number. This procedure is optional.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>authentication timer reauthenticate <code>seconds</code> Example: Device(config-if)# authentication timer reauthenticate 60</td>
<td>Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request. The range is 1 to 65535 seconds; the default is 5.</td>
</tr>
<tr>
<td>4</td>
<td>end Example: Device(config-if)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show authentication sessions interface <code>interface-id</code> Example: Device# show authentication sessions interface gigabitethernet2/0/1</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config Example: Device# copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Setting the Re-Authentication Number

You can also change the number of times that the switch restarts the authentication process before the port changes to the unauthorized state.

**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.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface gigabitethernet2/0/1</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> dot1x max-reauth-req count</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# dot1x max-reauth-req 5</td>
<td>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.</td>
</tr>
</tbody>
</table>

Returns to privileged EXEC mode.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Configuring IEEE 802.1x Port-Based Authentication

#### Enabling MAC Move

MAC move allows an authenticated host to move from one port on the switch to another.

Beginning in privileged EXEC mode, follow these steps to globally enable MAC move on the switch. This procedure is optional.

**Procedure**

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

| **Step 2**        | Enables MAC move on the switch. Default is deny. |
| authentication mac-move permit |         |
| Example:          | 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. |
| Device(config)# authentication mac-move permit | In legacy mode (IBNS 1.0), default value for **mac-move is deny** and in C3PL mode (IBNS 2.0) default value is **permit**. |
Enabling MAC Replace

MAC replace allows a host to replace an authenticated host on a port.

Beginning in privileged EXEC mode, follow these steps to enable MAC replace on an interface. This procedure is optional.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface gigabitethernet2/0/2</td>
<td></td>
</tr>
<tr>
<td>Step 3 authentication violation {protect</td>
<td>replace</td>
</tr>
<tr>
<td>Example:</td>
<td>The other keywords have these effects:</td>
</tr>
<tr>
<td>Device(config-if)# authentication</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>violation replace</td>
<td>• <strong>protect</strong>: the port drops packets with unexpected MAC addresses without generating a system message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>restrict</strong>: violating packets are dropped by the CPU and a system message is generated.</td>
</tr>
<tr>
<td></td>
<td>• <strong>shutdown</strong>: the port is error disabled when it receives an unexpected MAC address.</td>
</tr>
</tbody>
</table>

**Step 4**

**Example:**

Device(config-if)# end

Returns to privileged EXEC mode.

**Step 5**

**Example:**

Device# show running-config

Verifies your entries.

**Step 6**

**Example:**

Device# 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.

**Note**

In Cisco IOS XE Denali 16.3.x and Cisco IOS XE Everest 16.6.x, periodic AAA accounting updates are not supported. The switch does not send periodic interim accounting records to the accounting server. Periodic AAA accounting updates are available in Cisco IOS XE Fuji 16.9.x and later releases.

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:
### Configuring 802.1x Accounting

You must configure the RADIUS server to perform accounting tasks, such as logging start, stop, and interim-update messages and time stamps. To turn on these functions, enable logging of “Update/Watchdog packets from this AAA client” in your RADIUS server Network Configuration tab. Next, enable “CVS RADIUS Accounting” in your RADIUS server System Configuration tab.

Beginning in privileged EXEC mode, follow these steps to configure 802.1x accounting after AAA is enabled on your switch. This procedure is optional.

#### Procedure

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

When you configure a guest VLAN, clients that are not 802.1x-capable are put into the guest VLAN when the server does not receive a response to its EAP request/identity frame. Clients that are 802.1x-capable but that fail authentication are not granted network access. The switch supports guest VLANs in single-host or multiple-host mode.

Beginning in privileged EXEC mode, follow these steps to configure a guest VLAN. This procedure is optional.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface gigabitethernet 2/0/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Use one of the following:</td>
<td></td>
</tr>
<tr>
<td>• switchport mode access</td>
<td>• Sets the port to access mode.</td>
</tr>
<tr>
<td>• switchport mode private-vlan host</td>
<td>• Configures the Layer 2 port as a private-VLAN host port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# switchport mode private-vlan host</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring a Restricted VLAN

When you configure a restricted VLAN on a switch stack or a switch, clients that are IEEE 802.1x-compliant are moved into the restricted VLAN when the authentication server does not receive a valid username and password. The switch supports restricted VLANs only in single-host mode.

Beginning in privileged EXEC mode, follow these steps to configure a restricted VLAN. This procedure is optional.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# interface gigabitethernet 2/0/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Use one of the following: • switchport mode access • switchport mode private-vlan host</td>
<td>• Sets the port to access mode. • Configures the Layer 2 port as a private-VLAN host port.</td>
</tr>
<tr>
<td>Example: Device(config-if)# switchport mode access</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

#### Command or Action

- **Step 4**
  - `authentication port-control auto`
  - Example:
    ```
    Device(config-if)# authentication port-control auto
    ```

  **Purpose**: Enables 802.1x authentication on the port.

- **Step 5**
  - `authentication event fail action authorize vlan vlan-id`
  - Example:
    ```
    Device(config-if)# authentication event fail action authorize vlan 2
    ```

  **Purpose**: 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:
    ```
    Device(config-if)# end
    ```

  **Purpose**: 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.

#### Procedure

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

| **Step 2**        |         |
| `interface interface-id` | Specifies the port to be configured, and enter interface configuration mode. |
| Example:          |         |
| Devices(config)# interface gigabitethernet 2/0/3 |         |

<p>| <strong>Step 3</strong>        |         |
| Use one of the following: |         |
| • <code>switchport mode access</code> | • Sets the port to access mode. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• switchport mode private-vlan host</td>
<td>• Configures the Layer 2 port as a private-VLAN host port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# switchport mode access</td>
<td></td>
</tr>
</tbody>
</table>

Step 4

| authentication port-control auto | Enables 802.1x authentication on the port. |
| Example:                        |         |

Device(config-if)# authentication port-control auto

Step 5

| authentication event fail action authorize vlan vlan-id | 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. |
| Example:                                                 |         |

Device(config-if)# authentication event fail action authorize vlan 8

Step 6

| authentication event retry retry count | 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. |
| Example:                               |         |

Device(config-if)# authentication event retry 2

Step 7

| end | Returns to privileged EXEC mode. |
| Example: |         |

Device(config-if)# end

## Configuring 802.1x Inaccessible Authentication Bypass with Critical Voice VLAN

Beginning in privileged EXEC mode, follow these steps to configure critical voice VLAN on a port and enable the inaccessible authentication bypass feature.
## Procedure

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

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# aaa new-model</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>radius-server dead-criteria {time seconds} [tries number]</td>
<td>Sets the conditions that determine when a RADIUS server is considered unavailable or down (dead).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# radius-server dead-criteria time 20 tries 10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **time** — 1 to 120 seconds. The switch dynamically determines a default `seconds` value between 10 and 60.
- **number** — 1 to 100 tries. The switch dynamically determines a default `tries number` between 10 and 100.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>radius-server dead-time minutes</td>
<td>(Optional) Sets the number of minutes during which a RADIUS server is not sent requests. The range is from 0 to 1440 minutes (24 hours). The default is 0 minutes.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# radius-server dead-time 60</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>radius server server name</td>
<td>(Optional) Specifies the IP address of the RADIUS server.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# radius server rsim address ipv4 124.2.2.12</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>address {ipv4</td>
<td>ipv6} ip address auth-port port_number acct-port port_number</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-radius-server)# address ipv4 10.0.1.2 auth-port 1550 acct-port 1560</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
---|---
**Step 7** | **key string**  
*Example:*  
Device(config-radius-server)# key rad123  
(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.

**Step 8** | **exit**  
*Example:*  
Device(config-radius-server)# exit  
Exits the RADIUS server mode and enters the global configuration mode.

**Step 9** | **dot1x critical [eapol | recovery delay milliseconds]**  
*Example:*  
Device(config)# dot1x critical eapol  
Device(config)# dot1x critical recovery delay 2000  
(Optional) Configure the parameters for inaccessible authentication bypass:
- **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 10** | **interface interface-id**  
*Example:*  
Device(config)# interface gigabitethernet 1/0/1  
Specify the port to be configured, and enter interface configuration mode.

**Step 11** | **authentication event server dead action {authorize | reinitialize} vlan vlan-id**  
*Example:*  
Device(config-if)# authentication event server dead action authorize vlan 20  
Use these keywords to move hosts on the port if the RADIUS server is unreachable:
- **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.
### Command or Action

<table>
<thead>
<tr>
<th><strong>Step 12</strong></th>
<th><code>switchport voice vlan vlan-id</code></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-if)# switchport voice vlan vlan-id</code></td>
<td>Specifies the voice VLAN for the port. The voice VLAN cannot be the same as the critical data VLAN configured in Step 6.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 13</strong></th>
<th><code>authentication event server dead action authorize voice</code></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-if)# authentication event server dead action authorize voice</code></td>
<td>Configures critical voice VLAN to move data traffic on the port to the voice VLAN if the RADIUS server is unreachable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 14</strong></th>
<th><code>show authentication interface interface-id</code></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-if)# do show authentication interface gigabit 1/0/1</code></td>
<td>(Optional) Verify your entries.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 15</strong></th>
<th><code>copy running-config startup-config</code></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-if)# do copy running-config startup-config</code></td>
<td>(Optional) Verify your entries.</td>
</tr>
</tbody>
</table>

### Example

To return to the RADIUS server default settings, use the `no radius-server dead-criteria`, the `no radius-server deadtime`, and the `no radius server` global configuration commands. To disable inaccessible authentication bypass, use the `no authentication event server dead action` interface configuration command. To disable critical voice VLAN, use the `no authentication event server dead action authorize voice` interface configuration command.

### Example of Configuring Inaccessible Authentication Bypass

This example shows how to configure the inaccessible authentication bypass feature:

```
Device(config)# radius-server dead-criteria time 30 tries 20
Device(config)# radius-server deadtime 60
Device(config)# radius server server1
Device(config-radius-server)# address ipv4 172.29.36.49 acct-port 1618 auth-port 1612
Device(config-radius-server)# key abc1234
Device(config-radius-server)# exit
Device(config)# dot1x critical eapol
```

---

**Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)**

465
Configuring 802.1x Authentication with WoL

Beginning in privileged EXEC mode, follow these steps to enable 802.1x authentication with WoL. This procedure is optional.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# interface gigabitethernet2/0/3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> authentication control-direction {both</td>
<td>in}</td>
</tr>
<tr>
<td>Example: Device(config-if)# authentication control-direction both</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show authentication sessions interface</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>interface-id</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring MAC Authentication Bypass

Beginning in privileged EXEC mode, follow these steps to enable MAC authentication bypass. This procedure is optional.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# interface gigabitethernet 2/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 3 authentication port-control auto</td>
<td>Enables 802.1x authentication on the port.</td>
</tr>
<tr>
<td>Example: Device(config-if)# authentication port-control auto</td>
<td></td>
</tr>
<tr>
<td>Step 4 mab [eap]</td>
<td>Enables MAC authentication bypass. (Optional) Use the <strong>eap</strong> keyword to configure the switch to use EAP for authorization.</td>
</tr>
<tr>
<td>Example: Device(config-if)# mab</td>
<td></td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Configuring 802.1x User Distribution

Beginning in privileged EXEC mode, follow these steps to configure a VLAN group and to map a VLAN to it:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>vlan group vlan-group-name vlan-list</code></td>
<td>Configures a VLAN group, and maps a single VLAN or a range of VLANs to it.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# vlan group eng-dept</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>vlan-list 10</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# end</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>no vlan group vlan-group-name vlan-list</code></td>
<td>Clears the VLAN group configuration or elements of the VLAN group configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# no vlan group eng-dept</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>vlan-list 10</code></td>
<td></td>
</tr>
</tbody>
</table>

Example of Configuring VLAN Groups

This example shows how to configure the VLAN groups, to map the VLANs to the groups, to and verify the VLAN group configurations and mapping to the specified VLANs:

```
Device(config)# vlan group eng-dept vlan-list 10
Device(config)# show vlan group group-name eng-dept
Group Name       Vlans Mapped
---------------- ----------------
```
### Configuring NAC Layer 2 802.1x Validation

You can configure NAC Layer 2 802.1x validation, which is also referred to as 802.1x authentication with a RADIUS server.

Beginning in privileged EXEC mode, follow these steps to configure NAC Layer 2 802.1x validation. The procedure is optional.

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# interface gigabitethernet2/0/3</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>switchport mode access</td>
<td>Sets the port to access mode only if you configured the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# switchport mode access</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>authentication event no-response action authorize vlan vlan-id</td>
<td>Specifies an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# authentication event no-response action authorize vlan 8</td>
<td>You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN, or a voice VLAN as an 802.1x guest VLAN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>authentication periodic</td>
<td>Enables periodic re-authentication of the client, which is disabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# authentication periodic</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>authentication timer reauthenticate</td>
<td>Sets re-authentication attempt for the client (set to one hour). This command affects the behavior of the switch only if periodic re-authentication is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# authentication timer reauthenticate</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show authentication sessions interface interface-id</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show authentication sessions interface gigabitethernet2/0/3</td>
<td></td>
</tr>
</tbody>
</table>
Purpose

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

| Command or Action | Purpose |
|--- | ---
| configure terminal | Enters global configuration mode. |

| Command or Action | Purpose |
|--- | ---
| cisp enable | Enables CISP. |

| Command or Action | Purpose |
|--- | ---
| interface interface-id | Specifies the port to be configured, and enter interface configuration mode. |

| Command or Action | Purpose |
|--- | ---
| switchport mode access | Sets the port mode to access. |

### 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 authenticator switch interface configuration must be restored to access mode by explicitly flapping it if a line card is removed and inserted in the chassis when CISP or NEAT session is active.
- The `cisco-av-pairs` must be configured as `device-traffic-class=switch` on the ISE, which sets the interface as a trunk after the supplicant is successfully authenticated.

Beginning in privileged EXEC mode, follow these steps to configure a switch as an authenticator:

**Procedure**

| Command or Action | Purpose |
|--- | ---
<p>| configure terminal | Enters global configuration mode. |
| cisp enable | Enables CISP. |
| interface interface-id | Specifies the port to be configured, and enter interface configuration mode. |
| switchport mode access | Sets the port mode to access. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config-if)# switchport mode access</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>authentication port-control auto</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# authentication port-control auto</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>dot1x pae authenticator</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# dot1x pae authenticator</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>spanning-tree portfast</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# spanning-tree portfast trunk</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# end</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>show running-config interface interface-id</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# show running-config interface gigabitethernet 2/0/1</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# copy running-config startup-config</td>
</tr>
</tbody>
</table>

**Note**
Saving changes to the configuration file will mean that the authenticator interface will continue to be in trunk mode after reload. If you want the authenticator interface to remain as an access port, do not save your changes to the configuration file.
Configuring a Supplicant Switch with NEAT

Beginning in privileged EXEC mode, follow these steps to configure a switch as a supplicant:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>cispenable</td>
<td>Enables CISP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# cispenable</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>dot1x credentials profile</td>
<td>Creates 802.1x credentials profile. This must be attached to the port that is configured as supplicant.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# dot1x credentials test</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>username suppswitch</td>
<td>Creates a username.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# username suppswitch</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>password password</td>
<td>Creates a password for the new username.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# password myswitch</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>dot1x supplicant force-multicast</td>
<td>Forces the switch to send only multicast EAPOL packets when it receives either unicast or multicast packets. This also allows NEAT to work on the supplicant switch in all host modes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# dot1x supplicant force-multicast</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# interface gigabitethernet1/0/1</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>switchport trunk encapsulation dot1q</strong></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Sets the port to trunk mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>switchport mode trunk</strong></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Configures the interface as a VLAN trunk port.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>dot1x pae supplicant</strong></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Configures the interface as a port access entity (PAE) supplicant.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>dot1x credentials</strong></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Attaches the 802.1x credentials profile to the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>end</strong></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>show running-config interface</strong></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Verifies your configuration.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td><strong>copy running-config startup-config</strong></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Saves your entries in the configuration file.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>Configuring NEAT with Auto Smartports Macros</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>You can also use an Auto Smartports user-defined macro instead of the</td>
<td></td>
</tr>
</tbody>
</table>
Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs

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:

#### Before you begin

SISF-Based device tracking is a prerequisite to configuring 802.1x authentication. Ensure that you have enabled device tracking programmatically or manually. For more information, see the Configuring SISF-Based Tracking chapter.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>aaa authorization network default local group radius</td>
<td>Sets the authorization method to local. To remove the authorization method, use the no aaa authorization network default local group radius command.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# aaa authorization network default local group radius</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Downloadable Policy

Beginning in privileged EXEC mode:

**Before you begin**

SISF-Based device tracking is a prerequisite to configuring 802.1x authentication. Ensure that you have enabled device tracking programmatically or manually.

For more information, see *Configuring SISF-Based Tracking.*
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# <code>configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
| Step 2| `access-list access-list-number { deny | permit } { hostname | any | host } log` | Defines the default port ACL. The access-list-number 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 source is the source address of the network or host that sends a packet, such as this:  
  - **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.  
  (Optional) Applies the source-wildcard wildcard bits to the source.  
  (Optional) Enters log to cause an informational logging message about the packet that matches the entry to be sent to the console. |
|       | **Example:**                                           |                                                                                             |
|       | Device(config)# `access-list 1 deny any log`           |                                                                                             |
| Step 3| `interface interface-id`                               | Enters interface configuration mode.                                                       |
|       | **Example:**                                           |                                                                                             |
|       | Device(config)# `interface gigabitethernet2/0/2`        |                                                                                             |
| Step 4| `ip access-group acl-id in`                            | Configures the default ACL on the port in the input direction.                             |
|       | **Example:**                                           |                                                                                             |
|       | Device(config-if)# `ip access-group default_acl in`    |                                                                                             |
|       | **Note**                                               | The acl-id is an access list name or number.                                                |
Configuring IEEE 802.1x Port-Based Authentication

Beginning in privileged EXEC mode, follow these steps:

**Procedure**

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

**Configuring VLAN ID-based MAC Authentication**

Beginning in privileged EXEC mode, follow these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Step 6** aaa new-model

Example:

Device(config)# aaa new-model

**Step 7** aaa authorization network default group radius

Example:

Device(config)# aaa authorization network default group radius

**Step 8** radius-server vsa send authentication

Example:

Device(config)# radius-server vsa send authentication

**Step 9** end

Example:

Device(config)# end

Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)
### Configuring Flexible Authentication Ordering

The examples used in the instructions below change the order of Flexible Authentication Ordering so that MAB is attempted before IEEE 802.1X authentication (dot1x). MAB is configured as the first authentication method, so MAB will have priority over all other authentication methods.


Beginning in privileged EXEC mode, follow these steps:

#### Procedure

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

| **Step 2** interface interface-id | Specifies the port to be configured, and enter interface configuration mode. |
| Example:                        |         |
| Device(config)# interface gigabitethernet 1/0/1 |         |
### Configuring Open1x

Beginning in privileged EXEC mode, follow these steps to enable manual control of the port authorization state:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# interface</code></td>
<td></td>
</tr>
</tbody>
</table>

---

**Purpose**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Sets the port to access mode only if you previously configured the RADIUS server.</td>
</tr>
<tr>
<td><code>switchport mode access</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-if)# switchport mode access</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Sets the order of authentication methods used on a port.</td>
</tr>
<tr>
<td>`authentication order [ dot1x</td>
<td>mab ]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-if)# authentication order mab dot1x</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Adds an authentication method to the port-priority list.</td>
</tr>
<tr>
<td>`authentication priority [ dot1x</td>
<td>mab ]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-if)# authentication priority mab dot1x</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-if)# end</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>gigabitethernet 1/0/1</td>
<td>Sets the port to access mode only if you configured the RADIUS server.</td>
</tr>
<tr>
<td><strong>Step 3</strong> switchport mode access</td>
<td>Sets the port to access mode only if you configured the RADIUS server.</td>
</tr>
<tr>
<td><em>Example:</em> Device(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> authentication control-direction {both</td>
<td>in}</td>
</tr>
<tr>
<td><em>Example:</em> Device(config-if)# authentication control-direction both</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> authentication fallback name</td>
<td>(Optional) Configures a port to use web authentication as a fallback method for clients that do not support 802.1x authentication.</td>
</tr>
<tr>
<td><em>Example:</em> Device(config-if)# authentication fallback profile1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> authentication host-mode [multi-auth</td>
<td>multi-domain</td>
</tr>
<tr>
<td><em>Example:</em> Device(config-if)# authentication host-mode multi-auth</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> authentication open</td>
<td>(Optional) Enables or disable open access on a port.</td>
</tr>
<tr>
<td><em>Example:</em> Device(config-if)# authentication open</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> authentication order [dot1x</td>
<td>mab]</td>
</tr>
<tr>
<td><em>Example:</em> Device(config-if)# authentication order dot1x webauth</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> authentication periodic</td>
<td>(Optional) Enables or disable reauthentication on a port.</td>
</tr>
<tr>
<td><em>Example:</em> Device(config-if)# authentication</td>
<td></td>
</tr>
</tbody>
</table>
Disabling 802.1x Authentication on the Port

You can disable 802.1x authentication on the port by using the `no dot1x pae` interface configuration command. Beginning in privileged EXEC mode, follow these steps to disable 802.1x authentication on the port. This procedure is optional.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface gigabitethernet 2/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> switchport mode access</td>
<td>(Optional) Sets the port to access mode only if you configured the RADIUS server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no dot1x pae authenticator</td>
<td>Disables 802.1x authentication on the port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Resetting the 802.1x Authentication Configuration to the Default Values

Beginning in privileged EXEC mode, follow these steps to reset the 802.1x authentication configuration to the default values. This procedure is optional.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code></td>
<td>Enters interface configuration mode, and specify the port to be configured.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# interface gigabitethernet 1/0/2</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>dot1x default</code></td>
<td>Resets the 802.1x parameters to the default values.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-if)# dot1x default</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
Monitoring 802.1x Statistics and Status

Table 63: Privileged EXEC show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dot1x all statistics</td>
<td>Displays 802.1x statistics for all ports</td>
</tr>
<tr>
<td>show dot1x interface interface-id statistics</td>
<td>Displays 802.1x statistics for a specific port</td>
</tr>
<tr>
<td>show dot1x all [count</td>
<td>details</td>
</tr>
<tr>
<td>show dot1x interface interface-id</td>
<td>Displays the 802.1x administrative and operational status for a specific port</td>
</tr>
</tbody>
</table>

Table 64: Global Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no dot1x logging verbose</td>
<td>Filters verbose 802.1x authentication messages (beginning with Cisco IOS Release 12.2(55)SE)</td>
</tr>
</tbody>
</table>

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

Feature Information for IEEE 802.1x Port-Based Authentication

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 65: Feature Information for IEEE 802.1x Port-Based Authentication

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.1x Port-Based Authentication</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>IEEE 802.1x authentication prevents unauthorized devices (clients) from gaining access to the network.</td>
</tr>
</tbody>
</table>
Web-Based Authentication

This chapter describes how to configure web-based authentication on the device. It contains these sections:

- Web-Based Authentication Overview, on page 485
- How to Configure Web-Based Authentication, on page 494
- Verifying Web-Based Authentication Status, on page 506

Web-Based Authentication Overview

Use the web-based authentication feature, known as web authentication proxy, to authenticate end users on host systems that do not run the IEEE 802.1x supplicant.

Note

You can configure web-based authentication on Layer 2 and Layer 3 interfaces.

When you initiate an HTTP session, web-based authentication intercepts ingress HTTP packets from the host and sends an HTML login page to the users. The users enter their credentials, which the web-based authentication feature sends to the authentication, authorization, and accounting (AAA) server for authentication.

If authentication succeeds, web-based authentication sends a Login-Successful HTML page to the host and applies the access policies returned by the AAA server.

If authentication fails, web-based authentication forwards a Login-Fail HTML page to the user, prompting the user to retry the login. If the user exceeds the maximum number of attempts, web-based authentication forwards a Login-Expired HTML page to the host, and the user is placed on a watch list for a waiting period.

Note

HTTPS traffic interception for central web authentication redirect is not supported.
You should use global parameter-map (for method-type, custom, and redirect) only for using the same web authentication methods like consent, web consent, and webauth, for all the clients and SSIDs. This ensures that all the clients have the same web-authentication method.

If the requirement is to use Consent for one SSID and Web-authentication for another SSID, then you should use two named parameter-maps. You should configure Consent in first parameter-map and configure webauth in second parameter-map.

The traceback that you receive when webauth client tries to do authentication does not have any performance or behavioral impact. It happens rarely when the context for which FFM replied back to EPM for ACL application is already dequeued (possibly due to timer expiry) and the session becomes "unauthorized".

Based on where the web pages are hosted, the local web authentication can be categorized as follows:

- **Internal**—The internal default HTML pages (Login, Success, Fail, and Expire) in the controller are used during the local web authentication.
- **Customized**—The customized web pages (Login, Success, Fail, and Expire) are downloaded onto the controller and used during the local web authentication.
- **External**—The customized web pages are hosted on the external web server instead of using the in-built or custom web pages.

Based on the various web authentication pages, the types of web authentication are as follows:

- **Webauth**—This is a basic web authentication. Herein, the controller presents a policy page with the user name and password. You need to enter the correct credentials to access the network.
- **Consent or web-passsthrough**—Herein, the controller presents a policy page with the Accept or Deny buttons. You need to click the Accept button to access the network.
- **Webconsent**—This is a combination of webauth and consent web authentication types. Herein, the controller presents a policy page with Accept or Deny buttons along with username or password. You need to enter the correct credentials and click the Accept button to access the network.

**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.
Host Detection

The switch maintains an IP device tracking table to store information about detected hosts. For Layer 2 interfaces, web-based authentication detects IP hosts by using these mechanisms:

- ARP based trigger—ARP redirect ACL allows web-based authentication to detect hosts with a static IP address or a dynamic IP address.
- Dynamic ARP inspection
- DHCP snooping—Web-based authentication is notified when the switch creates a DHCP-binding entry for the host.

Session Creation

When web-based authentication detects a new host, it creates a session as follows:

- Reviews the exception list.
  If the host IP is included in the exception list, the policy from the exception list entry is applied, and the session is established.

- Reviews for authorization bypass
  If the host IP is not on the exception list, web-based authentication sends a nonresponsive-host (NRH) request to the server.
    If the server response is access accepted, authorization is bypassed for this host. The session is established.

- Sets up the HTTP intercept ACL
  If the server response to the NRH request is access rejected, the HTTP intercept ACL is activated, and the session waits for HTTP traffic from the host.

Authentication Process

When you enable web-based authentication, these events occur:

- The user initiates an HTTP session.
• The HTTP traffic is intercepted, and authorization is initiated. The switch sends the login page to the user. The user enters a username and password, and the switch sends the entries to the authentication server.

• If the authentication succeeds, the switch downloads and activates the user’s access policy from the authentication server. The login success page is sent to the user.

• If the authentication fails, the switch sends the login fail page. The user retries the login. If the maximum number of attempts fails, the switch sends the login expired page, and the host is placed in a watch list. After the watch list times out, the user can retry the authentication process.

• If the authentication server does not respond to the switch, and if an AAA fail policy is configured, the switch applies the failure access policy to the host. The login success page is sent to the user.

• The switch reauthenticates a client when the host does not respond to an ARP probe on a Layer 2 interface, or when the host does not send any traffic within the idle timeout on a Layer 3 interface.

• The feature applies the downloaded timeout or the locally configured session timeout.

---

**Note**

Beginning with Cisco IOS XE Denali 16.1.1 and later, the default session timeout value for web-based authentication on WLC is 1800 seconds. The default session timeout value was infinite seconds, prior to Cisco IOS XE Denali 16.1.1.

• If the terminate action is RADIUS, the feature sends a nonresponsive host (NRH) request to the server. The terminate action is included in the response from the server.

• If the terminate action is default, the session is dismantled, and the applied policy is removed.

---

**Local Web Authentication Banner**

With Web Authentication, you can create a default and customized web-browser banners that appears when you log in to a switch.

The banner appears on both the login page and the authentication-result pop-up pages. The default banner messages are as follows:

- **Authentication Successful**
- **Authentication Failed**
- **Authentication Expired**

The Local Web Authentication Banner can be configured in legacy CLIs as follows:

- Legacy mode—Use the `ip admission auth-proxy-banner http` global configuration command.
- New-style mode—Use the `parameter-map type webauth global banner` global configuration command.

The default banner *Cisco Systems* and *Switch host-name Authentication* appear on the Login Page. *Cisco Systems* appears on the authentication result pop-up page.
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.
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.


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.
- 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.
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.
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.

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.

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 (PAACL) as the default access policy for ingress traffic from hosts connected to the port. After authentication, the web-based authentication host policy overrides the PAACL. 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 66: Default Web-based Authentication Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Disabled</td>
</tr>
<tr>
<td>RADIUS server</td>
<td></td>
</tr>
<tr>
<td>• IP address</td>
<td>• None specified</td>
</tr>
<tr>
<td>• UDP authentication port</td>
<td>• None specified</td>
</tr>
<tr>
<td>• Key</td>
<td></td>
</tr>
<tr>
<td>Default value of inactivity timeout</td>
<td>3600 seconds</td>
</tr>
<tr>
<td>Inactivity timeout</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Web-Based Authentication Configuration Guidelines and Restrictions

• Web-based authentication is an ingress-only feature.
• You can configure web-based authentication only on access ports. Web-based authentication is not supported on trunk ports, EtherChannel member ports, or dynamic trunk ports.
• External web authentication, where the switch redirects a client to a particular host or web server for displaying login message, is not supported.
• You cannot authenticate hosts on Layer 2 interfaces with static ARP cache assignment. These hosts are not detected by the web-based authentication feature because they do not send ARP messages.
• You must enable SISF-Based device tracking to use web-based authentication. By default, SISF-Based device tracking is disabled on a switch.
• 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 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.

Note

You need to configure some settings on the RADIUS server, including: the switch IP address, the key string to be shared by both the server and the switch, and the downloadable ACL (DACL). For more information, see the RADIUS server documentation.

• When you upgrade from IOS XE release 3.6.x and 3.7.x, ensure that you use radius-server attribute wireless accounting call-station-id macaddress command to configure mac-address. This is because the accounting default call-station-id is changed from mac-address to IP address from Cisco IOS XE Denali 16.3.x onwards.
Configuring the Authentication Rule and Interfaces

Follow these steps to configure the authentication rule and interfaces:

Before you begin

SISF-Based device tracking is a prerequisite to Web Authentication. Ensure that you have enabled device tracking programmatically or manually.

For more information, see Configuring SISF-Based Tracking.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip admission name proxy http</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Configures an authentication rule for web-based authorization.</td>
</tr>
<tr>
<td>Device(config)# ip admission name webauth1 proxy http</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> interface type slot/port</td>
<td>Enters interface configuration mode and specifies the ingress Layer 2 or Layer 3 interface to be enabled for web-based authentication. type can be fastethernet, gigabit ethernet, or tengigabitethernet.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface gigabitethernet 1/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ip access-group name</td>
<td>Applies the default ACL.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ip access-group webauthag</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ip admission name</td>
<td>Configures an authentication rule for web-based authorization for the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring AAA Authentication

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device&gt; enable</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device# configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>aaa new-model</strong></td>
<td>Enables AAA functionality.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Device(config)# aaa new-model</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**aaa authentication login default group {tacacs+</td>
<td>radius}**</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# aaa authentication login default group tacacs+</td>
<td>named_authentication_list refers to any name that is not greater than 31 characters.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aaa authorization auth-proxy default group {tacacs+</td>
<td>Creates an authorization method list for web-based authorization.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>radius}</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# aaa authorization auth-proxy default group tacacs+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tacacs server server-name</td>
<td>Specifies an AAA server.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# tacacs server yourserver</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>address {ipv4</td>
<td>ipv6} ip address</td>
<td>Configures the IP address for the TACACS server.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-server-tacacs)# address ipv4 10.0.1.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>key string</td>
<td>Configures the authorization and encryption key used between the switch and the TACACS server.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-server-tacacs)# key cisco123</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits the TACACS server mode and enters the global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-server-tacacs)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td>Verifies your entries.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)
### Configuring Switch-to-RADIUS-Server Communication

Follow these steps to configure the RADIUS server parameters:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip radius source-interface</td>
<td>Specifies that the RADIUS packets have the IP address of the indicated interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip radius source-interface vlan 80</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>radius server server name</td>
<td>(Optional) Specifies the IP address of the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# radius server rsim address ipv4 124.2.2.12</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>address {ipv4</td>
<td>ipv6} ip address</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-radius-server)# address</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the HTTP Server

To use web-based authentication, you must enable the HTTP server within the Device. You can enable the server for either HTTP or HTTPS.

**Note**

The Apple psuedo-browser will not open if you configure only the `ip http secure-server` command. You should also configure the `ip http server` command.

Follow the procedure given below to enable the server for either HTTP or HTTPS:

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>ip http server</code></td>
<td></td>
</tr>
<tr>
<td><code>ip http secure-server</code></td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>key string</code></td>
<td>(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS server.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td>Device(config-radius-server)# key rad123</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits the RADIUS server mode and enters the global configuration mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td>Device(config-radius-server)# exit</td>
</tr>
<tr>
<td><code>radius-server dead-criteria tries num-tries</code></td>
<td>Specifies the number of unanswered sent messages to a RADIUS server before considering the server to be inactive. The range of <code>num-tries</code> is 1 to 100.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td>Device(config)# radius-server dead-criteria tries 30</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td>Device(config)# end</td>
</tr>
</tbody>
</table>
## Customizing the Authentication Proxy Web Pages

You can configure web authentication to display four substitute HTML pages to the user in place of the Device default HTML pages during web-based authentication.

Follow these steps to specify the use of your custom authentication proxy web pages:

### Before you begin

Store your custom HTML files on the Device flash memory.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

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.

### Command Table

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>ip http server</code></td>
<td>Enables the HTTP server. The web-based authentication feature uses the HTTP server to communicate with the hosts for user authentication.</td>
</tr>
<tr>
<td><code>ip http secure-server</code></td>
<td>Enables HTTPS. You can configure custom authentication proxy web pages or specify a redirection URL for successful login.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Customizing the Authentication Proxy Web Pages

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Example:**
Device> `enable` | • Enter your password if prompted. |
| **Step 2**
configure terminal | Enters global configuration mode. |
| **Example:**
Device# `configure terminal` | |
| **Step 3**
`ip admission proxy http login page file` `device:login-filename` | Specifies the location in the Device memory file system of the custom HTML file to use in place of the default login page. The `device:` is flash memory. |
| **Example:**
Device(config)# `ip admission proxy http login page file disk1:login.htm` | |
| **Step 4**
`ip admission proxy http success page file` `device:success-filename` | Specifies the location of the custom HTML file to use in place of the default login success page. |
| **Example:**
Device(config)# `ip admission proxy http success page file disk1:success.htm` | |
| **Step 5**
`ip admission proxy http failure page file` `device:fail-filename` | Specifies the location of the custom HTML file to use in place of the default login failure page. |
| **Example:**
Device(config)# `ip admission proxy http fail page file disk1:fail.htm` | |
| **Step 6**
`ip admission proxy http login expired page file` `device:expired-filename` | Specifies the location of the custom HTML file to use in place of the default login expired page. |
| **Example:**
Device(config)# `ip admission proxy http login expired page file disk1:expired.htm` | |
| **Step 7**
`end` | Returns to privileged EXEC mode. |
| **Example:**
Device(config)# `end` | |
Specifying a Redirection URL for Successful Login

Follow these steps to specify a URL to which the user is redirected after authentication, effectively replacing the internal Success HTML page:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

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

| **Step 3** ip admission proxy http success redirect url-string | Specifies a URL for redirection of the user in place of the default login success page. |
| Example:                                               |                                                                         |
| Device(config)# ip admission proxy http success redirect www.example.com |                                                                         |

| **Step 4** end                           | Returns to privileged EXEC mode.                                        |
| Example:                                |                                                                         |
| Device(config)# end                     |                                                                         |

Configuring the Web-Based Authentication Parameters

Follow these steps to configure the maximum number of failed login attempts before the client is placed in a watch list for a waiting period:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Web-Based Authentication Local Banner

Follow these steps to configure a local banner on a switch that has web authentication configured.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
</tbody>
</table>
| `enable`          | Enables privileged EXEC mode.  
| `Device> enable`  | • Enter your password if prompted. |
| `configure terminal` | Enters global configuration mode. |
| `Device# configure terminal` | |
| **Step 2**        | **Command or Action** |
| `ip admission max-login-attempts number` | Sets the maximum number of failed login attempts. The range is 1 to 2147483647 attempts. The default is 5. |
| `Device(config)# ip admission max-login-attempts 10` | |
| **Step 3**        | **Purpose** |
| `end`              | Returns to privileged EXEC mode. |
| `Device(config)# end` | |
| **Step 4**        | **Command or Action** |
| `show running-config` | Verifies your entries. |
| `Device# show running-config` | |
| **Step 5**        | **Command or Action** |
| `copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |
| `Device# copy running-config startup-config` | |
Purpose

---

Command or Action | Purpose
--- | ---
Device# configure terminal |  

**Step 3**

ip admission auth-proxy-banner http [banner-text | file-path]

*Example:*

Device(config)# ip admission auth-proxy-banner http C My Switch C

Enables the local banner.
(Optional) Create a custom banner by entering `C banner-text C` (where `C` is a delimiting character), or `file-path` that indicates a file (for example, a logo or text file) that appears in the banner.

**Step 4**

end

*Example:*

Device(config)# end

Returns to privileged EXEC mode.

**Step 5**

show running-config

*Example:*

Device# show running-config

Verifies your entries.

**Step 6**

copy running-config startup-config

*Example:*

Device# copy running-config startup-config

(Optional) Saves your entries in the configuration file.

---

**Removing Web-Based Authentication Cache Entries**

Follow these steps to remove web-based authentication cache entries:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**

enable

*Example:*

Device> enable

Enables privileged EXEC mode.

- Enter your password if prompted.

| **Step 2**

clear ip auth-proxy cache { * | host ip address }

*Example:*

Device# clear ip auth-proxy cache

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. |
Verifying 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 67: Privileged EXEC show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show authentication sessions method webauth</td>
<td>Displays the web-based authentication settings for all interfaces for fastethernet, gigabitethernet, or tengigabitethernet</td>
</tr>
<tr>
<td>show authentication sessions interface type slot/port[details]</td>
<td>Displays the web-based authentication settings for the specified interface for fastethernet, gigabitethernet, or tengigabitethernet. In Session Aware Networking mode, use the show access-session interface command.</td>
</tr>
</tbody>
</table>
Overview of Port-Based Traffic Control

Port-based traffic control is a set of Layer 2 features on the Cisco Catalyst switches used to filter or block packets at the port level in response to specific traffic conditions. The following port-based traffic control features are supported:

- Storm Control
- Protected Ports
- Port Blocking
- Port Security
- Protocol Storm Protection

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

Figure 35: Broadcast Storm Control Example

This example shows broadcast traffic patterns on an interface over a given period of time.

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.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td><code>Device&gt;</code> <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>interface interface-id</code></td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# interface gigabitethernet1/0/1</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Configures broadcast, multicast, or unicast storm control. By default, storm control is disabled.

The keywords have these meanings:

- **For level**, 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 **level-low**, 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.

- For **bps bps**, 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 **bps-low**, 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 pps**, 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.

### Command or Action

| Step 4 | storm-control {broadcast | multicast | unicast} level {level [level-low] | bps bps [bps-low] | pps pps [pps-low]}
| --- | --- |

**Example:**

```
Device(config-if)# storm-control unicast
level 87 65
```
### Configuring Port-Based Traffic Control

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• (Optional) For <strong>pps-low</strong>, 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 <strong>0.0</strong> to <strong>10000000000.0</strong>. For BPS and PPS settings, you can use metric suffixes such as k, m, and g for large number thresholds.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 5

**storm-control action {shutdown | trap}**

Specifies the action to be taken when a storm is detected. The default is to filter out the traffic and not to send traps.

- 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.

**Example:**

```
Device(config-if)# storm-control action trap
```

### Step 6

**end**

Returns to privileged EXEC mode.

**Example:**

```
Device(config-if)# end
```

### Step 7

**show storm-control [interface-id] [broadcast | multicast | unicast]**

Verifies the storm control suppression levels set on the interface for the specified traffic type. If you do not enter a traffic type, details for all traffic types (broadcast, multicast and unicast) are displayed.

**Example:**

```
Device# show storm-control gigabitethernet1/0/1 unicast
```

### Step 8

**copy running-config startup-config**

(Optional) Saves your entries in the configuration file.

**Example:**

```
Device# copy running-config startup-config
```

---

### 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.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
  Example:  
  Device> enable |
| Step 2 | configure terminal | Enters global configuration mode.  
  Example:  
  Device# configure terminal |
| Step 3 | errdisable detect cause small-frame | Enables the small-frame rate-arrival feature on the switch.  
  Example:  
  Device(config)# errdisable detect cause small-frame |
| Step 4 | errdisable recovery interval interval | (Optional) Specifies the time to recover from the specified error-disabled state.  
  Example:  
  Device(config)# errdisable recovery interval 60 |
| Step 5 | errdisable recovery cause small-frame | (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  
  Example:  
  Device(config)# errdisable recovery cause small-frame |
| Step 6 | interface interface-id | Enters interface configuration mode, and specify the interface to be configured.  
  Example:  
  Device(config)# interface gigabitethernet1/0/2 |
| Step 7 | small-frame violation-rate pps | 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)  
  Example:  
  Device(config)# small-frame violation-rate 1000
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-if)# small-frame violation rate 10000</td>
<td></td>
</tr>
</tbody>
</table>

**Step 8**

```
Device(config)# end
```

Returns to privileged EXEC mode.

**Step 9**

```
Device(config)# show interfaces interface-id
```

Example:

```
Device# show interfaces gigabitethernet1/0/2
```

Verifies the configuration.

**Step 10**

```
Device# show running-config
```

Example:

```
Device# show running-config
```

Verifies your entries.

**Step 11**

```
Device# copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.

---

**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.
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.

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.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; <strong>enable</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# <strong>configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# <strong>interface gigabitethernet 1/0/1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>switchport protected</code></td>
<td>Configures the interface to be a protected port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# <strong>switchport protected</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# <strong>end</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Monitoring Protected Ports

#### Table 68: Commands for Displaying Protected Port Settings

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces [interface-id] switchport</code></td>
<td>Displays the administrative and operational status of all switching (nonrouting) ports or the specified port, including port blocking and port protection settings.</td>
</tr>
</tbody>
</table>

### 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.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | `enable`          | Enables privileged EXEC mode.  
  *Example:*  
  ```console
  Device> enable
  ``` |
| 2    | `configure terminal` | Enters global configuration mode.  
  *Example:*  
  ```console
  Device# configure terminal
  ``` |
| 3    | `interface interface-id` | Specifies the interface to be configured, and enter interface configuration mode.  
  *Example:*  
  ```console
  Device(config)# interface gigabitethernet 1/0/1
  ``` |
| 4    | `switchport block multicast` | Blocks unknown multicast forwarding out of the port.  
  *Example:*  
  ```console
  Device(config-if)# switchport block multicast
  ``` |
| 5    | `switchport block unicast` | Blocks unknown unicast forwarding out of the port.  
  *Example:*  
  ```console
  Device(config-if)# switchport block unicast
  ``` |
| 6    | `end` | Returns to privileged EXEC mode.  
  *Example:*  
  ```console
  Device(config)# end
  ``` |
### Monitoring Port Blocking

**Table 69: Commands for Displaying Port Blocking Settings**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces [interface-id] switchport</code></td>
<td>Displays the administrative and operational status of all switching (nonrouting) ports or the specified port, including port blocking and port protection settings.</td>
</tr>
</tbody>
</table>

### 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 is set by the maximum number of available MAC addresses allowed in the system. 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.

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.
Running diagnostic tests with port security enabled.

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.

  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 shutdown` 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 70: Security Violation Mode Actions**

<table>
<thead>
<tr>
<th>Violation Mode</th>
<th>Traffic is forwarded</th>
<th>Sends SNMP trap</th>
<th>Sends syslog message</th>
<th>Displays error message</th>
<th>Violation counter increments</th>
<th>Shuts down port</th>
</tr>
</thead>
<tbody>
<tr>
<td>protect</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>restrict</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>shutdown</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>shutdown vlan</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

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.

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 71: Default Port Security Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port security</td>
<td>Disabled on a port.</td>
</tr>
<tr>
<td>Sticky address learning</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Maximum number of secure MAC addresses per port</td>
<td>1.</td>
</tr>
<tr>
<td>Violation mode</td>
<td>Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.</td>
</tr>
<tr>
<td>Port security aging</td>
<td>Disabled. Aging time is 0.</td>
</tr>
</tbody>
</table>

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).

- Voice VLAN is only supported on access ports and not on trunk ports, even though the configuration is allowed.

- 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 72: Port Security Compatibility with Other Switch Features**

<table>
<thead>
<tr>
<th>Type of Port or Feature on Port</th>
<th>Compatible with Port Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTP port</td>
<td>No</td>
</tr>
<tr>
<td>Trunk port</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic-access port</td>
<td>No</td>
</tr>
<tr>
<td>Routed port</td>
<td>No</td>
</tr>
<tr>
<td>SPAN source port</td>
<td>Yes</td>
</tr>
<tr>
<td>SPAN destination port</td>
<td>No</td>
</tr>
<tr>
<td>EtherChannel</td>
<td>Yes</td>
</tr>
<tr>
<td>Tunneling port</td>
<td>Yes</td>
</tr>
<tr>
<td>Protected port</td>
<td>Yes</td>
</tr>
<tr>
<td>IEEE 802.1x port</td>
<td>Yes</td>
</tr>
<tr>
<td>Voice VLAN port</td>
<td>Yes</td>
</tr>
<tr>
<td>IP source guard</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic Address Resolution Protocol (ARP) inspection</td>
<td>Yes</td>
</tr>
<tr>
<td>Flex Links</td>
<td>Yes</td>
</tr>
</tbody>
</table>

15 DTP=Dynamic Trunking Protocol
16 A port configured with the `switchport mode dynamic` interface configuration command.
A VLAN Query Protocol (VQP) port configured with the `switchport access vlan dynamic` interface configuration command.

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.

### Overview of Port-Based Traffic Control

Port-based traffic control is a set of Layer 2 features on the Cisco Catalyst switches used to filter or block packets at the port level in response to specific traffic conditions. The following port-based traffic control features are supported in the Cisco IOS Release for which this guide is written:

- Storm Control
- Protected Ports
- Port Blocking
- Port Security
- Protocol Storm Protection

### 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:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device&gt; enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>interface interface-id</code></td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# interface gigabitethernet1/0/1</code></td>
<td></td>
</tr>
</tbody>
</table>
## Purpose

**Command or Action**

| Step 4 | `switchport mode {access | trunk}` |
|--------|-----------------------------------|
| Example: | `Device(config-if)# switchport mode access` |

Sets the interface switchport mode as access or trunk; an interface in the default mode (dynamic auto) cannot be configured as a secure port.

<table>
<thead>
<tr>
<th>Step 5</th>
<th><code>switchport voice vlan vlan-id</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Device(config-if)# switchport voice vlan 22</code></td>
</tr>
</tbody>
</table>

Enables voice VLAN on a port.

**Note**

 vlan-id—Specifies the VLAN to be used for voice traffic.

<table>
<thead>
<tr>
<th>Step 6</th>
<th><code>switchport port-security</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Device(config-if)# switchport port-security</code></td>
</tr>
</tbody>
</table>

Enable port security on the interface.

**Note**

Under certain conditions, when port security is enabled on the member ports in a switch stack, the DHCP and ARP packets would be dropped. To resolve this, configure a shut and no shut on the interface.

| Step 7 | `switchport port-security [maximum value [vlan {vlan-list | {access | voice}]}]]` |
|--------|-----------------------------------------------------------------|
| Example: | `Device(config-if)# switchport port-security maximum 20` |

(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 the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.

(Optional) vlan—Sets a per-VLAN maximum value

Enter one of these options after you enter the `vlan` keyword:

- `vlan-list`—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.
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.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport port-security violation {protect</td>
<td>restrict</td>
</tr>
</tbody>
</table>

- **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.

  **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.

- **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,
Purpose

Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport port-security {mac-address mac-address [vlan {vlan-id</td>
<td>access</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
</tbody>
</table>

Step 9

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.

Example:

Device(config-if)# switchport port-security mac-address 00:A0:C7:12:C9:25 vlan 3 voice

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. |

(Optional) vlan—sets a per-VLAN maximum value.

Enter one of these options after you enter the vlan keyword:

• 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.
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.

**Step 10**

```
switchport port-security mac-address sticky
```

*(Optional)* Enables sticky learning on the interface.

```
Device(config-if)# switchport port-security mac-address sticky
```

**Step 11**

```
switchport port-security mac-address sticky {mac-address | vlan {vlan-id | {access | voice}}}}
```

*(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.

```
Device(config-if)# switchport port-security mac-address sticky 00:A0:C7:12:C9:25 vlan voice
```

*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.

*(Optional)* `vlan`—sets a per-VLAN maximum value.

Enter one of these options after you enter the `vlan` keyword:

- `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.

*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.
### 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.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>· Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling and Configuring Port Security Aging

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 13**       | **Command or Action** |
| show port-security| Verifies your entries. |
| Example:          | |
| Device# show port-security | |

| **Step 14**       | **Command or Action** |
| show running-config| Verifies your entries. |
| Example:          | |
| Device# show running-config | |

| **Step 15**       | **Command or Action** |
| copy running-config startup-config | (Optional) Saves your entries in the configuration file. |
| Example:          | |
| Device# copy running-config startup-config | |
### Enabling and Configuring Port Security Aging

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config)# interface gigabitethernet1/0/1</code></td>
<td>Enables or disable static aging for the secure port, or set the aging time or type.</td>
</tr>
</tbody>
</table>

**Step 4**

```
switchport port-security aging {static | time time | type {absolute | inactivity}}
```

**Example:**

```
Device(config-if)# switchport port-security aging time 120
```

- **Note**: The switch does not support port security aging of sticky secure addresses.

Enter *static* to enable aging for statically configured secure addresses on this port.

For *time*, specifies the aging time for this port. The valid range is from 0 to 1440 minutes.

For *type*, select one of these keywords:

- **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:**

```
Device(config)# end
```

Returns to privileged EXEC mode.

**Step 6**

```
show port-security [interface interface-id] [address]
```

**Example:**

```
Device# show port-security interface gigabitethernet1/0/1
```

Verifies your entries.

**Step 7**

```
show running-config
```

**Example:**

```
Device# show running-config
```

Verifies your entries.
### 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.

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 50
Device(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:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(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).

```
Device(config)# interface tengigabitethernet1/0/1
Device(config-if)# switchport access vlan 21
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan 22
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 20
Device(config-if)# switchport port-security violation restrict
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Device(config-if)# switchport port-security mac-address 0000.0000.0003
Device(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Device(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Device(config-if)# switchport port-security maximum 10 vlan access
Device(config-if)# switchport port-security maximum 10 vlan voice
```
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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Port-Based Traffic Control

#### Monitoring Protocol Storm Protection

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

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>psp {arp</td>
<td>dhcp</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# psp dhcp pps 35</td>
<td>For value, 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>errdisable detect cause psp</td>
<td>(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.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# errdisable detect cause psp</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>errdisable recovery interval time</td>
<td>(Optional) Configures an auto-recovery time (in seconds) for error-disabled virtual ports. When a virtual port is error-disabled, the switch auto-recover after this time. The range is from 30 to 86400 seconds.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show psp config {arp</td>
<td>dhcp</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# show psp config dhcp</td>
<td></td>
</tr>
</tbody>
</table>

### Monitoring Protocol Storm Protection

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show psp config {arp</td>
<td>dhcp</td>
</tr>
</tbody>
</table>
Additional References for Port-Based Traffic Control

MIBs

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

Technical Assistance

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

Feature Information for Port-Based Traffic Control

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 73: Feature Information for Port-Based Traffic Control

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-Based Traffic Control</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>Port-based traffic control is a set of Layer 2 features on the Cisco Catalyst switches used to filter or block packets at the port level in response to specific traffic conditions.</td>
</tr>
</tbody>
</table>
Restrictions for CoPP

Restrictions for control plane policing (CoPP) include the following:

- Only ingress CoPP is supported. The system-cpp-policy policy-map is available on the control plane interface, and only in the ingress direction.

- Only the system-cpp-policy policy-map can be installed on the control plane interface.

- The system-cpp-policy policy-map and the system-defined classes cannot be modified or deleted.

- Only the police action is allowed under the system-cpp-policy policy-map. The police rate for system-defined classes must be configured only in packets per second (pps); for user-defined class maps this must be configured only in bits per second (bps).

- When setting the policer rate, note that a clock frequency limitation causes differences in the default rate and the set rate values displayed for some classes (even if you set the default rate for all classes). See the User-Configurable Aspects of CoPP and Example: Setting the Default Policer Rates for All CPU Queues topics in this chapter for more information.

- Removing the policer rate configuration, disables CoPP on all affected queues.

- The show run command does not display information about classes configured under system-cpp policy, when they are left at default values. Use the show policy-map system-cpp-policy or the show policy-map control-plane commands instead.

You can continue use the show run command to display information about custom policies.
Information About Control Plane Policing

This chapter describes how control plane policing (CoPP) works on your device and how to configure it.

CoPP Overview

The CoPP feature improves security on your device protecting the CPU from unnecessary traffic and DoS attacks. It can also protect control and management traffic from traffic drops caused by high volumes of other, lower priority traffic.

Your device is typically segmented into three planes of operation, each with its own objective:

- The data plane, to forward data packets.
- The control plane, to route data correctly.
- The management plane, to manage network elements.

You can use CoPP to protect most of the CPU-bound traffic and ensure routing stability, reachability, and packet delivery. Most importantly, you can use CoPP to protect the CPU from a DoS attack.

CoPP uses the modular QoS command-line interface (MQC) and CPU queues to achieve these objectives. Different types of control plane traffic are grouped together based on certain criteria, and assigned to a CPU queue. You can manage these CPU queues by configuring dedicated policers in hardware. For example, you can modify the policer rate for certain CPU queues (traffic-type), or you can disable the policer for a certain type of traffic.

Although the policers are configured in hardware, CoPP does not affect CPU performance or the performance of the data plane. But since it limits the number of packets going to CPU, the CPU load is controlled. This means that services waiting for packets from hardware may see a more controlled rate of incoming packets (the rate being user-configurable).

System-Defined Aspects of CoPP

When you power-up the device for the first time, the system automatically performs the following tasks:

- Looks for policy-map `system-cpp-policy`. If not found, the system creates and installs it on the control-plane.
- Creates eighteen class-maps under `system-cpp-policy`.
  
  The next time you power-up the device, the system detects the policy and class maps that have already been created.

- Enables all CPU queues by default, with their respective default rate. The default rates are indicated in the table System-Defined Values for CoPP.

The following table lists the class-maps that the system creates when you load the device. It lists the policer that corresponds to each class-map and one or more CPU queues that are grouped under each class-map. There is a one-to-one mapping of class-maps to policers; and one or more CPU queues map to a class-map.
### Table 74: System-Defined Values for CoPP

<table>
<thead>
<tr>
<th>Class Maps Names</th>
<th>Policer Index (Policer No.)</th>
<th>CPU queues (Queue No.)</th>
<th>Default Policer Rate (pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>system-cp-police-data</td>
<td>WK_CPU_POLICE_DATA(0)</td>
<td>WK_CPU_Q_ICMP_GEN(3)</td>
<td>600</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WK_CPU_Q_BROADCAST(12)</td>
<td>600</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WK_CPU_Q_ICMP_REDIRECT(6)</td>
<td>600</td>
</tr>
<tr>
<td>system-cp-police-l2-control</td>
<td>WK_CPU_POLICE_L2_CONTROL(1)</td>
<td>WK_CPU_Q_L2_CONTROL(1)</td>
<td>2000</td>
</tr>
<tr>
<td>system-cp-police-routing-control</td>
<td>WK_CPU_ROUTING_CONTROL(4)</td>
<td>WK_CPU_Q_ROUTING_CONTROL(4)</td>
<td>5400</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WK_CPU_Q_LOW_LATENCY(27)</td>
<td>5400</td>
</tr>
<tr>
<td>system-cp-police-punt-webauth</td>
<td>WK_CPU_POLICE_PUNT_WEBAUTH(7)</td>
<td>WK_CPU_Q_PUNT_WEBAUTH(22)</td>
<td>1000</td>
</tr>
<tr>
<td>system-cp-police-topology-control</td>
<td>WK_CPU_TOPOLOGY_CONTROL(15)</td>
<td>WK_CPU_Q_TOPOLOGY_CONTROL(15)</td>
<td>13000</td>
</tr>
<tr>
<td>system-cp-police-multicast</td>
<td>WK_CPU_MULTICAST(20)</td>
<td>WK_CPU_Q_TRANSIT_TRAFFIC(18)</td>
<td>500</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WK_CPU_Q_MCAST_DATA(30)</td>
<td>500</td>
</tr>
<tr>
<td>system-cp-police-sys-data</td>
<td>WK_CPU_POLICE_SYS_DATA (10)</td>
<td>WK_CPU_Q_OPENFLOW (13)</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WK_CPU_Q_CRYPTOCONTROL(23)</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WK_CPU_Q_EXCEPTION(24)</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WK_CPU_Q_EGR_EXCEPTION(28)</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WK_CPU_Q_NFL_SAMPLED_DATA(26)</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WK_CPU_Q_GOLD_PKT(31)</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WK_CPU_Q_RPF_FAILED(19)</td>
<td>100</td>
</tr>
<tr>
<td>system-cp-police-dot1x-auth</td>
<td>WK_CPU_DOT1X_AUTH(0)</td>
<td>WK_CPU_Q_DOT1X_AUTH(0)</td>
<td>1000</td>
</tr>
<tr>
<td>system-cp-police-protocol-snooping</td>
<td>WK_CPU_PROTO_SNOOPING(16)</td>
<td>WK_CPU_Q_PROTO_SNOOPING(16)</td>
<td>2000</td>
</tr>
<tr>
<td>system-cp-police-dhcp-snooping</td>
<td>WK_CPU_DHCP_SNOOPING</td>
<td>WK_CPU_Q_DHCP_SNOOPING(17)</td>
<td>500</td>
</tr>
<tr>
<td>system-cp-police-sw-forward</td>
<td>WK_CPU_SW_FORWARDING(13)</td>
<td>WK_CPU_Q_SW_FORWARDING(14)</td>
<td>1000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WK_CPU_Q_LOGGING(21)</td>
<td>1000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WK_CPU_Q_L2_IVX_DATA_PACKET(11)</td>
<td>1000</td>
</tr>
<tr>
<td>system-cp-police-forus</td>
<td>WK_CPU_FORUS(14)</td>
<td>WK_CPU_Q_FORUS_ADDRESS_RESOLUTION(8)</td>
<td>4000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WK_CPU_Q_FORUS_TRAFFIC(2)</td>
<td>4000</td>
</tr>
</tbody>
</table>
When you upgrade or downgrade the software version on your device, note the following:

- When upgrading from one software release to another:

  The upgrade could be from one Cisco IOS XE 16.x.x release to another Cisco IOS XE 16.x.x release:
  
  - If the device did not have a `system-cpp-policy` policy map before upgrade, then on upgrade, a default policy is created.
  
  - If the device had a `system-cpp-policy` policy map before upgrade, then on upgrade, the policy is not re-generated. Enter the `cpp system-default` command in global configuration mode to get the default policy working.

    **Note**
    
    We recommend that you to enter the `cpp system-default` command after any major upgrade to get the latest, default policer rates.

- When downgrading from one software release to another:

  The downgrade could be from one Cisco IOS XE 16.x.x release to another Cisco IOS XE 16.x.x release:

  - The `system-cpp-policy` policy map is retained on the device, but not installed on the control plane. You can delete the policy.

  - If you downgrade to an earlier release and then upgrade to a later release:
    
    - If you delete the policy after downgrading to an earlier Cisco IOS XE 16.x.x and then upgrade to a Cisco IOS XE 16.x.x release, the policy is generated with defaults.
    
    - If you do not delete the policy after downgrade to an earlier Cisco IOS XE 16.x.x release, then on upgrade to a later Cisco IOS XE 16.x.x release, the policy is not regenerated.

    Enter the `cpp system-default` command in global configuration mode to get the default policy working.
User-Configurable Aspects of CoPP

You can perform these tasks to manage control plane traffic:

---

**Note**

All `system-cpp-policy` configurations must be saved so they are retained after reboot.

---

**Enable or Disable a Policer for CPU Queues**

Enable a policer for a CPU queue, by configuring a policer action (in packets per second) under the corresponding class-map, within the `system-cpp-policy policy-map`.

Disable a policer for CPU queue, by removing the policer action under the corresponding class-map, within the `system-cpp-policy policy-map`.

---

**Note**

If a default policer is already present, carefully consider and control its removal; otherwise the system may see a CPU hog or other anomalies, such as control packet drops.

---

**Change the Policer Rate**

You can do this by configuring a policer rate action (in packets per second), under the corresponding class-map, within the `system-cpp-policy policy-map`.

When setting a policer rate, note that the rate you set is automatically converted to the nearest multiple of 200. For instance, if you set the policer rate of a CPU queue 100 pps, the system changes it to 200; or if set the policer rate to 650, the system changes it to 600. See Example: Setting the Default Policer Rates for All CPU Queues in this chapter, for sample output that displays this behavior.

---

**Set Policer Rates to Default**

Set the policer for CPU queues to their default values, by entering the `cpp system-default` command in global configuration mode.

---

**Create User-Defined Class Maps**

If a given traffic class does not have a designated class map, and you want to protect this traffic, you can create specific class maps (with filters) for such traffic packets and add these user-defined class maps to `system-cpp-policy`.

While `system-cpp-policy` is applied in the ingress direction, the forwarding engine driver (FED) changes policers on user-defined class maps to the egress. The filters and the policers in all user-defined classes must therefore be applied as egress classifications and actions, respectively. The policy map itself is unaffected by this change in the direction.

When you add a user-defined class map to `system-cpp-policy`, the system automatically installs it on all 32 CPU queues (in addition to the control plane), resulting in 33 instances of the policy. You can see this by entering the command in privileged EXEC mode.

The police rate on these class maps is controlled by the Active Queue Management (AQM) policer. AQM provides buffering control of traffic flows prior to queuing a packet into the transmit queue of a port, ensuring...
that certain flows do not hog the switch packet memory. If the AQM policer feature is enabled, any user-defined police rates exceeding the AQM policer limits are disregarded.

User-defined class maps have normal QoS or ACL classification filters.

## How to Configure CoPP

### Enabling a CPU Queue or Changing the Policer Rate

The procedure to enable a CPU queue and change the policer rate of a CPU queue is the same. Follow these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>policy-map policy-map-name</td>
<td>Enters the policy map configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# policy-map system-cpp-policy</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>class class-name</td>
<td>Enters the class action configuration mode. Enter the name of the class that corresponds to the CPU queue you want to enable. See table <em>System-Defined Values for CoPP</em>.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-pmap)# class system-cpp-police-protocol-snooping</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>police rate rate pps</td>
<td>Specifies an upper limit on the number of incoming packets processed per second, for the specified traffic class. <strong>Note</strong> The rate you specify is applied to all CPU queues that belong to the class-map you have specified.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-pmap-c)# police rate 100 pps</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Returns to the global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-pmap-c-police)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-pmap-c)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-pmap)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)#</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong> control-plane</td>
<td>Enters the control plane (config-cp) configuration mode</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# control-plane</td>
<td></td>
</tr>
<tr>
<td>Device(config-cp)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> service-policy input policy-name</td>
<td>Installs system-cpp-policy in FED. This command is required for you to see the FED policy. Not configuring this command will lead to an error.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# control-plane</td>
<td></td>
</tr>
<tr>
<td>Device(config-cp)# service-policy input system-cpp-policy</td>
<td></td>
</tr>
<tr>
<td>Device(config-cp)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong> end</td>
<td>Returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-cp)# end</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong> show policy-map control-plane</td>
<td>Displays all the classes configured under system-cpp policy, the rates configured for the various traffic types, and statistics</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# show policy-map control-plane</td>
<td></td>
</tr>
</tbody>
</table>

---

### Disabling a CPU Queue

Follow these steps to disable a CPU queue:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

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

**Command or Action**

Device# configure terminal

**Step 3**

**policy-map** *policy-map-name*

**Example:**

Device(config)# policy-map system-cpp-policy
Device(config-pmap)#

**Step 4**

**class** *class-name*

**Example:**

Device(config-pmap)# class system-cpp-police-protocol-snooping
Device(config-pmap-c)#

**Step 5**

**no police rate** *rate* pps

**Example:**

Device(config-pmap-c)# no police rate 100 pps

**Step 6**

**end**

**Example:**

Device(config-pmap-c)# end

**Step 7**

**show policy-map control-plane**

**Example:**

Device# show policy-map control-plane

### Setting the Default Policer Rates for All CPU Queues

Follow these steps to set the policer rates for all CPU queues to their default rates:

**Procedure**

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

Device> enable
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>cpp system-default</td>
<td>Sets the policer rates for all the classes to the default rate.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# cpp system-default</td>
<td>Defaulting CPP: Policer rate for all classes will be set to their defaults</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# end</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>show platform hardware fed {active</td>
<td>standby} qos queue stats internal cpu policer</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show platform hardware fed active qos queue stats internal cpu policer</td>
<td></td>
</tr>
</tbody>
</table>

**Creating A User-Defined Class Map**

Follow these steps to create user-defined class maps in system-cpp-policy and set the policer rates in bps

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>3</td>
<td><code>class-map class-map-name</code></td>
<td>Specify the class you want to create. Enters the class map configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# class-map example_class</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-cmap)#</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>exit</code></td>
<td>Exits the class map configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-cmap)# exit</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)#</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>policy-map policy-map-name</code></td>
<td>Enter the policy map name. Enters the policy map configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# policy-map system-cpp-policy</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-pmap)#</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>class-map class-map-name</code></td>
<td>Enters the class action configuration mode. Enter the name of the class.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-pmap)# class example_class</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-pmap-c)#</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>[no] police rate target_bit_rate</code></td>
<td>Specifies the bit rate per second, enter a value between 8000 and 10000000000.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-pmap-c)# police 90000</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>The police rate for user-defined class-maps must not exceed 10000 pps worth of traffic.</td>
</tr>
<tr>
<td>8</td>
<td><code>end</code></td>
<td>Returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-pmap-c-police)# end</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device#</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>show policy-map control-plane</code></td>
<td>Displays all the classes configured under system-cpp policy, including the user-defined class maps, and the rates configured.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# show policy-map control-plane</code></td>
<td></td>
</tr>
</tbody>
</table>
Examples for Configuring CoPP

Example: Enabling a CPU Queue or Changing the Policier Rate of a CPU Queue

This example shows how to enable a CPU queue or to change the policier rate of a CPU queue. Here the class `system-cpp-police-protocol-snooping` CPU queue is enabled with the policier rate of 2000 pps.

```
Device> enable
Device# configure terminal
Device(config)# policy-map system-cpp-policy
Device(config-pmap)# class system-cpp-police-protocol-snooping
Device(config-pmap-c)# police rate 2000 pps
Device(config-pmap-c-police)# end

Device# show policy-map control-plane
Control Plane

Service-policy input: system-cpp-policy

<output truncated>

Class-map: system-cpp-police-dot1x-auth (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: none
  police:
    rate 1000 pps, burst 244 packets
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop

Class-map: system-cpp-police-protocol-snooping (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: none
  police:
    rate 2000 pps, burst 488 packets
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop

<output truncated>

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any
```
Example: Disabling a CPU Queue

This example shows how to disable a CPU queue. Here the class `system-cpp-police-protocol-snooping` CPU queue is disabled.

Example: Setting the Default Policer Rates for All CPU Queues

This example shows how to set the policer rates for all CPU queues to their default and then verify the setting.

Note

For some CPU queues, the default rate and the set rate values will not be the same, even if you set the default rate for all classes. This because the set rate is rounded off to the nearest multiple of 200. This behavior is controlled by the clock speed of your device. In the sample output below, the default and set rate values for DHCP Snooping and NFL SAMPLED DATA display this difference.

Device> enable
Device# configure terminal
Device(config)# cpp system-default
Defaulting CPP : Policer rate for all classes will be set to their defaults
Device(config)# end

Device# show platform hardware fed active qos queue stats internal cpu policer

CPU Queue Statistics

<table>
<thead>
<tr>
<th>QId</th>
<th>PlcIdx</th>
<th>Queue Name</th>
<th>Enabled</th>
<th>(default) Rate</th>
<th>(set) Rate</th>
<th>Queue Drop(Bytes)</th>
<th>Queue Drop(Frames)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>11</td>
<td>DOT1X Auth</td>
<td>Yes</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>L2 Control</td>
<td>Yes</td>
<td>2000</td>
<td>2000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
<td>Forus traffic</td>
<td>Yes</td>
<td>4000</td>
<td>4000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>ICMP GEN</td>
<td>Yes</td>
<td>600</td>
<td>600</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>Routing Control</td>
<td>Yes</td>
<td>5400</td>
<td>5400</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>14</td>
<td>Forus Address resolution</td>
<td>Yes</td>
<td>4000</td>
<td>4000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>ICMP Redirect</td>
<td>Yes</td>
<td>600</td>
<td>600</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>16</td>
<td>Inter FED Traffic</td>
<td>Yes</td>
<td>2000</td>
<td>2000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>L2 LVX Cont Pack</td>
<td>Yes</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>16</td>
<td>EWLC Control</td>
<td>Yes</td>
<td>2000</td>
<td>2000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>16</td>
<td>EWLC Data</td>
<td>Yes</td>
<td>2000</td>
<td>2000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>13</td>
<td>L2 LVX Data Pack</td>
<td>Yes</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>BRÓADCAST</td>
<td>Yes</td>
<td>600</td>
<td>600</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>10</td>
<td>Openflow</td>
<td>Yes</td>
<td>100</td>
<td>200</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Example: Setting the Default Policer Rates for All CPU Queues

* NOTE: CPU queue policer rates are configured to the closest hardware supported value
Example: Creating a User-Defined Class Map

Device

This example shows how to create a user-defined class map, apply it to system-cpp-policy and display information about where the policy is applied.

A user-defined class map is applied to system-cpp-policy, which means that any control traffic matching the user-defined class map class-cpp-user is subject to the aggregate policer, under the user-defined class map. Statistics for the user defined traffic class are reported in Bytes.

Device> enable
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# class-map match-any class-cpp-user
Device(config-cmap)# match dscp cs1
Device(config-cmap)# exit
Device(config)# policy-map system-cpp-policy
Device(config-pmap)# class class-cpp-user
Device(config-pmap-c)# police rate 2m bps
Device(config-pmap-c-policer)# end

Device# show policy-map control-plane
Class-map: class-cpp-user (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match:  dscp cs1 (8)
  police:
    rate 2000000 bps, burst 62500 bytes
    conformed 0 bytes; actions: transmit
    exceeded 0 bytes; actions: drop
    conformed 0000 bps, exceeded 0000 bps

When you add a user-defined class map to `system-cpp-policy`, the system automatically installs it on all 32 CPU queues, in addition to the control plane (resulting in 33 instances of the policy).

Note how the direction is display as egress (OUT), even though `system-cpp-policy` is applied in the ingress

```
Device# show platform software fed switch active qos policy target status

TCG status summary:

<table>
<thead>
<tr>
<th>Loc</th>
<th>Interface</th>
<th>IIF-ID</th>
<th>Dir</th>
<th>State: (cfg, opr)</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:0</td>
<td>CoPP-Queue-0</td>
<td>0x00000001000001</td>
<td>OUT</td>
<td>VALID, SET_INHW</td>
<td>system-cpp-policy</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-1</td>
<td>0x00000001000002</td>
<td>OUT</td>
<td>VALID, SET_INHW</td>
<td>system-cpp-policy</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-2</td>
<td>0x00000001000003</td>
<td>OUT</td>
<td>VALID, SET_INHW</td>
<td>system-cpp-policy</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-3</td>
<td>0x00000001000004</td>
<td>OUT</td>
<td>VALID, SET_INHW</td>
<td>system-cpp-policy</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-4</td>
<td>0x00000001000005</td>
<td>OUT</td>
<td>VALID, SET_INHW</td>
<td>system-cpp-policy</td>
</tr>
</tbody>
</table>

Monitoring CoPP

Use these commands to display policer settings, such as, traffic types and policer rates (user-configured and default rates) for CPU queues:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show policy-map control-plane</code></td>
<td>Displays the rates configured for the various traffic types</td>
</tr>
<tr>
<td><code>show policy-map system-cpp-policy</code></td>
<td>Displays all the classes configured under system-cpp policy, and policer rates</td>
</tr>
</tbody>
</table>
Feature History for Control Plane Policing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Plane Policing (CoPP) or CPP</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Change in the system behavior for policer rates that are set.</td>
<td>Cisco IOS XE Everest 16.6.4</td>
<td>For some CPU queues, the default rate and the set rate values will not be the same, even if you set the default rate for all classes. This because the set rate is rounded off to the nearest multiple of 200.</td>
</tr>
<tr>
<td>Changes in system-defined values for CoPP</td>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This new system-defined class was introduced: system-cpp-police-dhcp-snooping. This new CPU queue was added to the existing system-cpp-default class: WK_CPU_Q_INTER_FED_TRAFFIC. These CPU queues are no longer available: • WK_CPU_Q_SHOW_FORWARD • WK_CPU_Q_UNUSED. The default policer rate (pps) for some CPU queues has changed: • The default rate for WK_CPU_Q_EXCEPTION(24) was changed to 100 • The default rate for all the CPU queues under system-cpp-default was increased to 2000. • The default rate for all the CPU queues under system-cpp-police-forus was increased to 4000.</td>
</tr>
</tbody>
</table>
CHAPTER 27

Configuring Authorization and Revocation of Certificates in a PKI

Prerequisites for Authorization and Revocation of Certificates

Plan Your PKI Strategy

Tip
It is strongly recommended that you plan your entire PKI strategy before you begin to deploy actual certificates.

Authorization and revocation can occur only after you or a network administrator have completed the following tasks:

• Configured the certificate authority (CA).
• Enrolled peer devices with the CA.
• Identified and configured the protocol (such as IP Security [IPsec] or secure socket layer [SSL]) that is to be used for peer-to-peer communication.

You should decide which authorization and revocation strategy you are going to configure before enrolling peer devices because the peer device certificates might have to contain authorization and revocation-specific information.

High Availability

For high availability, IPsec-secured Stream Control Transmission Protocol (SCTP) must be configured on both the active and the standby routers. For synchronization to work, the redundancy mode on the certificate servers must be set to ACTIVE/STANDBY after you configure SCTP.
Restrictions for Authorization and Revocation of Certificates

- Depending on your Cisco IOS release, Lightweight Directory Access Protocol (LDAP) is supported.

Information About Authorization and Revocation of Certificates

PKI Authorization

PKI authentication does not provide authorization. Current solutions for authorization are specific to the router that is being configured, although a centrally managed solution is often required.

There is not a standard mechanism by which certificates are defined as authorized for some tasks and not for others. This authorization information can be captured in the certificate itself if the application is aware of the certificate-based authorization information. But this solution does not provide a simple mechanism for real-time updates to the authorization information and forces each application to be aware of the specific authorization information embedded in the certificate.

When the certificate-based ACL mechanism is configured as part of the trustpoint authentication, the application is no longer responsible for determining this authorization information, and it is no longer possible to specify for which application the certificate is authorized. In some cases, the certificate-based ACL on the router gets so large that it cannot be managed. Additionally, it is beneficial to retrieve certificate-based ACL indications from an external server.

Current solutions to the real-time authorization problem involve specifying a new protocol and building a new server (with associated tasks, such as management and data distribution).

PKI and AAA Server Integration for Certificate Status

Integrating your PKI with an authentication, authorization, and accounting (AAA) server provides an alternative online certificate status solution that leverages the existing AAA infrastructure. Certificates can be listed in the AAA database with appropriate levels of authorization. For components that do not explicitly support PKI-AAA, a default label of “all” from the AAA server provides authorization. Likewise, a label of “none” from the AAA database indicates that the specified certificate is not valid. (The absence of any application label is equivalent, but “none” is included for completeness and clarity). If the application component does support PKI-AAA, the component may be specified directly; for example, the application component could be “ipsec,” “ssl,” or “osp.” (ipsec=IP Security, ssl=Secure Sockets Layer, and osp=Open Settlement Protocol.)

Note

Currently, no application component supports specification of the application label.

- There may be a time delay when accessing the AAA server. If the AAA server is not available, the authorization fails.

RADIUS or TACACS+ Choosing a AAA Server Protocol

The AAA server can be configured to work with either the RADIUS or TACACS+ protocol. When you are configuring the AAA server for the PKI integration, you must set the RADIUS or TACACS attributes that are required for authorization.

If the RADIUS protocol is used, the password that is configured for the username in the AAA server should be set to “cisco,” which is acceptable because the certificate validation provides authentication and the AAA
database is only being used for authorization. When the TACACS protocol is used, the password that is configured for the username in the AAA server is irrelevant because TACACS supports authorization without requiring authentication (the password is used for authentication).

In addition, if you are using TACACS, you must add a PKI service to the AAA server. The custom attribute “cert-application=all” is added under the PKI service for the particular user or user group to authorize the specific username.

**Attribute-Value Pairs for PKI and AAA Server Integration**

The table below lists the attribute-value (AV) pairs that are to be used when setting up PKI integration with a AAA server. (Note the values shown in the table are possible values.) The AV pairs must match the client configuration. If they do not match, the peer certificate is not authorized.

<table>
<thead>
<tr>
<th>AV Pair</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco-avpair=pki:cert-application=all</td>
<td>Valid values are “all” and “none.”</td>
</tr>
<tr>
<td>cisco-avpair=pki:cert-trustpoint=msca</td>
<td>The value is a Cisco IOS command-line interface (CLI) configuration trustpoint label.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The cert-trustpoint AV pair is normally optional. If it is specified, the Cisco IOS router query must be coming from a certificate trustpoint that has a matching label, and the certificate that is authenticated must have the specified certificate serial number.</td>
</tr>
<tr>
<td>cisco-avpair=pki:cert-serial=16318DB7000100001671</td>
<td>The value is a certificate serial number.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The cert-serial AV pair is normally optional. If it is specified, the Cisco IOS router query must be coming from a certificate trustpoint that has a matching label, and the certificate that is authenticated must have the specified certificate serial number.</td>
</tr>
</tbody>
</table>

---

**Note** Users can sometimes have AV pairs that are different from those of every other user. As a result, a unique username is required for each user. The **all** parameter (within the **authorization username** command) specifies that the entire subject name of the certificate will be used as the authorization username.

---

**Table 75: AV Pairs That Must Match**
CRLs or OCSP Server Choosing a Certificate Revocation Mechanism

After a certificate is validated as a properly signed certificate, a certificate revocation method is performed to ensure that the certificate has not been revoked by the issuing CA. Cisco IOS software supports two revocation mechanisms--certificate revocation lists (CRLs) and Online Certificate Status Protocol (OCSP). Cisco IOS software also supports AAA integration for certificate checking; however, additional authorization functionality is included. For more information on PKI and AAA certificate authorization and status check, see the PKI and AAA Server Integration for Certificate Status section.

The following sections explain how each revocation mechanism works:

What Is a CRL

A certificate revocation list (CRL) is a list of revoked certificates. The CRL is created and digitally signed by the CA that originally issued the certificates. The CRL contains dates for when each certificate was issued and when it expires.

CAs publish new CRLs periodically or when a certificate for which the CA is responsible has been revoked. By default, a new CRL is downloaded after the currently cached CRL expires. An administrator may also configure the duration for which CRLs are cached in router memory or disable CRL caching completely. The CRL caching configuration applies to all CRLs associated with a trustpoint.

When the CRL expires, the router deletes it from its cache. A new CRL is downloaded when a certificate is presented for verification; however, if a newer version of the CRL that lists the certificate under examination is on the server but the router is still using the CRL in its cache, the router does not know that the certificate has been revoked. The certificate passes the revocation check even though it should have been denied.

When a CA issues a certificate, the CA can include in the certificate the CRL distribution point (CDP) for that certificate. Cisco IOS client devices use CDPs to locate and load the correct CRL. The Cisco IOS client supports multiple CDPs, but the Cisco IOS CA currently supports only one CDP; however, third-party vendor CAs may support multiple CDPs or different CDPs per certificate. If a CDP is not specified in the certificate, the client device uses the default Simple Certificate Enrollment Protocol (SCEP) method to retrieve the CRL. (The CDP location can be specified through the cdp-url command.)

When implementing CRLs, you should consider the following design considerations:

- CRL lifetimes and the security association (SA) and Internet Key Exchange (IKE) lifetimes.
• The CRL lifetime determines the length of time between CA-issued updates to the CRL. The default CRL lifetime value, which is 168 hours [1 week], can be changed through the `lifetime crl` command.

• The method of the CDP determines how the CRL is retrieved; some possible choices include HTTP, Lightweight Directory Access Protocol (LDAP), SCEP, or TFTP. HTTP, TFTP, and LDAP are the most commonly used methods. Although Cisco IOS software defaults to SCEP, an HTTP CDP is recommended for large installations using CRLs because HTTP can be made highly scalable.

• The location of the CDP determines from where the CRL is retrieved; for example, you can specify the server and file path from which to retrieve the CRL.

**Querying All CDPs During Revocation Check**

When a CDP server does not respond to a request, the Cisco IOS software reports an error, which may result in the peer’s certificate being rejected. To prevent a possible certificate rejection and if there are multiple CDPs in a certificate, the Cisco IOS software will attempt to use the CDPs in the order in which they appear in the certificate. The router will attempt to retrieve a CRL using each CDP URL or directory specification. If an error occurs using a CDP, an attempt will be made using the next CDP.

**Tip**

Although the Cisco IOS software will make every attempt to obtain the CRL from one of the indicated CDPs, it is recommended that you use an HTTP CDP server with high-speed redundant HTTP servers to avoid application timeouts because of slow CDP responses.

**What Is OCSP**

OCSP is an online mechanism that is used to determine certificate validity and provides the following flexibility as a revocation mechanism:

• OCSP can provide real-time certificate status checking.

• OCSP allows the network administrator to specify a central OCSP server, which can service all devices within a network.

• OCSP also allows the network administrator the flexibility to specify multiple OCSP servers, either per client certificate or per group of client certificates.

• OCSP server validation is usually based on the root CA certificate or a valid subordinate CA certificate, but may also be configured so that external CA certificates or self-signed certificates may be used. Using external CA certificates or self-signed certificates allows the OCSP servers certificate to be issued and validated from an alternative PKI hierarchy.

A network administrator can configure an OCSP server to collect and update CRLs from different CA servers. The devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every peer. When peers have to check the revocation status of a certificate, they send a query to the OCSP server that includes the serial number of the certificate in question and an optional unique identifier for the OCSP request, or a nonce. The OCSP server holds a copy of the CRL to determine if the CA has listed the certificate as being revoked; the server then responds to the peer including the nonce. If the nonce in the response from the OCSP server does not match the original nonce sent by the peer, the response is considered invalid and certificate verification fails. The dialog between the OCSP server and the peer consumes less bandwidth than most CRL downloads.

If the OCSP server is using a CRL, CRL time limitations will be applicable; that is, a CRL that is still valid might be used by the OCSP server although a new CRL has been issued by the CRL containing additional
certificate revocation information. Because fewer devices are downloading the CRL information on a regular basis, you can decrease the CRL lifetime value or configure the OCSP server not to cache the CRL. For more information, check your OCSP server documentation.

Note

OCSP multiple response handling: Support has been enabled for handling of multiple OCSP single responses from an OCSP responder in a response packet. In addition to the debug log messages the following debug log message will be displayed:

CRYPTO_PKI: Number of single Responses in OCSP response: 1 (this value can change depending upon the number of responses).

When to Use an OCSP Server

OCSP may be more appropriate than CRLs if your PKI has any of the following characteristics:

• Real-time certificate revocation status is necessary. CRLs are updated only periodically and the latest CRL may not always be cached by the client device. For example, if a client does not yet have the latest CRL cached and a newly revoked certificate is being checked, that revoked certificate will successfully pass the revocation check.

• There are a large number of revoked certificates or multiple CRLs. Caching a large CRL consumes large portions of Cisco IOS memory and may reduce resources available to other processes.

• CRLs expire frequently, causing the CDP to handle a larger load of CRLs.

When to Use Certificate-Based ACLs for Authorization or Revocation

Certificates contain several fields that are used to determine whether a device or user is authorized to perform a specified action.

Because certificate-based ACLs are configured on the device, they do not scale well for large numbers of ACLs; however, certificate-based ACLs do provide very granular control of specific device behavior. Certificate-based ACLs are also leveraged by additional features to help determine when PKI components such as revocation, authorization, or a trustpoint should be used. They provide a general mechanism allowing users to select a specific certificate or a group of certificates that are being validated for either authorization or additional processing.

Certificate-based ACLs specify one or more fields within the certificate and an acceptable value for each specified field. You can specify which fields within a certificate should be checked and which values those fields may or may not have.

There are six logical tests for comparing the field with the value—equal, not equal, contains, does not contain, less than, and greater than or equal. If more than one field is specified within a single certificate-based ACL, the tests of all of the fields within the ACL must succeed to match the ACL. The same field may be specified multiple times within the same ACL. More than one ACL may be specified, and ACL will be processed in turn until a match is found or all of the ACLs have been processed.

Ignore Revocation Checks Using a Certificate-Based ACL

Certificate-based ACLs can be configured to instruct your router to ignore the revocation check and expired certificates of a valid peer. Thus, a certificate that meets the specified criteria can be accepted regardless of the validity period of the certificate, or if the certificate meets the specified criteria, revocation checking does
not have to be performed. You can also use a certificate-based ACL to ignore the revocation check when the communication with a AAA server is protected with a certificate.

**Ignoring Revocation Lists**

To allow a trustpoint to enforce CRLs except for specific certificates, enter the `match certificate` command with the `skip revocation-check` keyword. This type of enforcement is most useful in a hub-and-spoke configuration in which you also want to allow direct spoke-to-spoke connections. In pure hub-and-spoke configurations, all spokes connect only to the hub, so CRL checking is necessary only on the hub. For one spoke to communicate directly with another spoke, the `match certificate` command with the `skip revocation-check` keyword can be used for neighboring peer certificates instead of requiring a CRL on each spoke.

**Ignoring Expired Certificates**

To configure your router to ignore expired certificates, enter the `match certificate` command with the `allow expired-certificate` keyword. This command has the following purposes:

- If the certificate of a peer has expired, this command may be used to “allow” the expired certificate until the peer can obtain a new certificate.

- If your router clock has not yet been set to the correct time, the certificate of a peer will appear to be not yet valid until the clock is set. This command may be used to allow the certificate of the peer even though your router clock is not set.

---

**Note**

If Network Time Protocol (NTP) is available only via the IPSec connection (usually via the hub in a hub-and-spoke configuration), the router clock can never be set. The tunnel to the hub cannot be “brought up” because the certificate of the hub is not yet valid.

- “Expired” is a generic term for a certificate that is expired or that is not yet valid. The certificate has a start and end time. An expired certificate, for purposes of the ACL, is one for which the current time of the router is outside the start and end times specified in the certificate.

**Skipping the AAA Check of the Certificate**

If the communication with an AAA server is protected with a certificate, and you want to skip the AAA check of the certificate, use the `match certificate` command with the `skip authorization-check` keyword. For example, if a virtual private network (VPN) tunnel is configured so that all AAA traffic goes over that tunnel, and the tunnel is protected with a certificate, you can use the `match certificate` command with the `skip authorization-check` keyword to skip the certificate check so that the tunnel can be established.

The `match certificate` command and the `skip authorization-check` keyword should be configured after PKI integration with an AAA server is configured.

---

**Note**

If the AAA server is available only via an IPSec connection, the AAA server cannot be contacted until after the IPSec connection is established. The IPSec connection cannot be “brought up” because the certificate of the AAA server is not yet valid.
PKI Certificate Chain Validation

A certificate chain establishes a sequence of trusted certificates --from a peer certificate to the root CA certificate. Within a PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trustpoint.

When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate, or trustpoint, is reached. An administrator may configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates.

Configuring the level to which a certificate chain is processed allows for the reauthentication of trusted certificates, the extension of a trusted certificate chain, and the completion of a certificate chain that contains a gap.

Reauthentication of Trusted Certificates

The default behavior is for the router to remove any trusted certificates from the certificate chain sent by the peer before the chain is validated. An administrator may configure certificate chain path processing so that the router does not remove CA certificates that are already trusted before chain validation, so that all certificates in the chain are re-authenticated for the current session.

Extending the Trusted Certificate Chain

The default behavior is for the router to use its trusted certificates to extend the certificate chain if there are any missing certificates in the certificate chain sent by the peer. The router will validate only certificates in the chain sent by the peer. An administrator may configure certificate chain path processing so that the certificates in the peer’s certificate chain and the router’s trusted certificates are validated to a specified point.

Completing Gaps in a Certificate Chain

An administrator may configure certificate chain processing so that if there is a gap in the configured Cisco IOS trustpoint hierarchy, certificates sent by the peer can be used to complete the set of certificates to be validated.

Note

If the trustpoint is configured to require parent validation and the peer does not provide the full certificate chain, the gap cannot be completed and the certificate chain is rejected and invalid.

Note

It is a configuration error if the trustpoint is configured to require parent validation and there is no parent trustpoint configured. The resulting certificate chain gap cannot be completed and the subordinate CA certificate cannot be validated. The certificate chain is invalid.

How to Configure Authorization and Revocation of Certificates for Your PKI

Configuring PKI Integration with a AAA Server

Perform this task to generate a AAA username from the certificate presented by the peer and specify which fields within a certificate should be used to build the AAA database username.
The following restrictions should be considered when using the all keyword as the subject name for the authorization username command:

- Some AAA servers limit the length of the username (for example, to 64 characters). As a result, the entire certificate subject name cannot be longer than the limitation of the server.

- Some AAA servers limit the available character set that may be used for the username (for example, a space [ ] and an equal sign [=] may not be acceptable). You cannot use the all keyword for a AAA server having such a character-set limitation.

- The subject-name command in the trustpoint configuration may not always be the final AAA subject name. If the fully qualified domain name (FQDN), serial number, or IP address of the router are included in a certificate request, the subject name field of the issued certificate will also have these components. To turn off the components, use the fqdn, serial-number, and ip-address commands with the none keyword.

- CA servers sometimes change the requested subject name field when they issue a certificate. For example, CA servers of some vendors switch the relative distinguished names (RDNs) in the requested subject names to the following order: CN, OU, O, L, ST, and C. However, another CA server might append the configured LDAP directory root (for example, O=cisco.com) to the end of the requested subject name.

- Depending on the tools you choose for displaying a certificate, the printed order of the RDNs in the subject name could be different. Cisco IOS software always displays the least significant RDN first, but other software, such as Open Source Secure Socket Layer (OpenSSL), does the opposite. Therefore, if you are configuring a AAA server with a full distinguished name (DN) (subject name) as the corresponding username, ensure that the Cisco IOS software style (that is, with the least significant RDN first) is used.

or

```
radius-server host  hostname  [key  string]
```

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt;enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>aaa new-model</td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# aaa new-model</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Authorization and Revocation of Certificates in a PKI

#### Configuring PKI Integration with a AAA Server

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>aaa authorization network listname [method]</code></td>
<td>Sets the parameters that restrict user access to a network.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# aaa authorization network maxaaa group tacacs+</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>crypto pki trustpoint name</code></td>
<td>Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# crypto pki trustpoint msca</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>enrollment [mode] [retry period minutes] [retry count number] url url [pem]</code></td>
<td>Specifies the following enrollment parameters of the CA:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(ca-trustpoint)# enrollment url http://caserver.myexample.com</code></td>
<td>(Optional) The <code>mode</code> keyword specifies the registration authority (RA) mode, if your CA system provides an RA. By default, RA mode is disabled.</td>
</tr>
<tr>
<td><code>- or-</code></td>
<td></td>
</tr>
<tr>
<td><code>Device(ca-trustpoint)# enrollment url http://2001:DB8:1:1::1:80</code></td>
<td>(Optional) The <code>retry period</code> keyword and <code>minutes</code> argument specifies the period, in minutes, in which the router waits before sending the CA another certificate request. Valid values are from 1 to 60. The default is 1.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>An IPv6 address can be added to the <code>http: enrolment</code> method. For example: <code>http://[ipv6-address]:80</code>. The IPv6 address must be enclosed in brackets in the URL.</td>
<td></td>
</tr>
<tr>
<td><code>- or-</code></td>
<td></td>
</tr>
<tr>
<td><code>Device(ca-trustpoint)# enrollment url</code></td>
<td>(Optional) The <code>pem</code> keyword adds privacy-enhanced mail (PEM) boundaries to the certificate request.</td>
</tr>
</tbody>
</table>

---

**Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)**
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td>(Optional) Checks the revocation status of a certificate.</td>
</tr>
<tr>
<td>revocation-check method</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(ca-trustpoint)# revocation-check crl</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Exits ca-trustpoint configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(ca-trustpoint)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Sets parameters for the different certificate fields that are used to build the AAA username.</td>
</tr>
<tr>
<td>authorization username</td>
<td>subjectname</td>
</tr>
<tr>
<td><strong>subjectname</strong></td>
<td>Sets the AAA authorization list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# authorization username subjectname serialnumber</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Specifies the AAA authorization list.</td>
</tr>
<tr>
<td>authorization list</td>
<td>listname</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# authorization list listname</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command/Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config)# authorization list maxaaa</code></td>
<td>Specifies a TACACS+ host. or Specifies a RADIUS host.</td>
</tr>
</tbody>
</table>

#### Step 11

**tacacs-server host** hostname [key string]

**Example:**

```
Device(config)# tacacs-server host 192.0.2.2 key a_secret_key
```

**radius-server host hostname [key string]**

**Example:**

```
Device(config)# radius-server host 192.0.2.1 key another_secret_key
```

---

### Troubleshooting Tips

To display debug messages for the trace of interaction (message type) between the CA and the router, use the `debug crypto pki transactions` command. (See the sample output, which shows a successful PKI integration with AAA server exchange and a failed PKI integration with AAA server exchange.)

#### Successful Exchange

```
Device# debug crypto pki transactions
Apr 22 23:15:03.695: CRYPTO_PKI: Found a issuer match
Apr 22 23:15:03.955: CRYPTO_PKI: cert revocation status unknown.
Apr 22 23:15:03.955: CRYPTO_PKI: Certificate validated without revocation check

Each line that shows “CRYPTO_PKI_AAA” indicates the state of the AAA authorization checks. Each of the AAA AV pairs is indicated, and then the results of the authorization check are shown.

Apr 22 23:15:04.019: CRYPTO_PKI_AAA: checking AAA authorization (ipsecca_script_aalist, PKI AAA-L, <all>)
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-application" = “all”)
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = “CA1”)
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-serial" = “15DE”)
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: parsed cert-lifetime-end as: 21:30:00
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: timezone specific extended
```

#### Failed Exchange

```
Device# debug crypto pki transactions
Apr 22 23:11:13.703: CRYPTO_PKI_AAA: checking AAA authorization =
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-application" = “all”)
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint"= “CA1”)
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: parsed cert-lifetime-end as: 21:30:00
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end is expired
```

In the above failed exchange, the certificate has expired.

### Configuring a Revocation Mechanism for PKI Certificate Status Checking

Perform this task to set up a CRL as the certificate revocation mechanism--CRLs or OCSP--that is used to check the status of certificates in a PKI.

#### The revocation-check Command

Use the `revocation-check` command to specify at least one method (OCSP, CRL, or skip the revocation check) that is to be used to ensure that the certificate of a peer has not been revoked. For multiple methods, the order in which the methods are applied is determined by the order specified via this command.

If your router does not have the applicable CRL and is unable to obtain one or if the OCSP server returns an error, your router will reject the peer’s certificate--unless you include the `none` keyword in your configuration. If the `none` keyword is configured, a revocation check will not be performed and the certificate will always be accepted.

#### Nonces and Peer Communications with OCSP Servers

When using OCSP, nonces, unique identifiers for OCSP requests, are sent by default during peer communications with your OCSP server. The use of nonces offers a more secure and reliable communication channel between the peer and OCSP server.

If your OCSP server does not support nonces, you may disable the sending of nonces. For more information, check your OCSP server documentation.

#### Before you begin

- Before issuing any client certificates, the appropriate settings on the server (such as setting the CDP) should be configured.
- When configuring an OCSP server to return the revocation status for a CA server, the OCSP server must be configured with an OCSP response signing certificate that is issued by that CA server. Ensure that the signing certificate is in the correct format, or the router will not accept the OCSP response. See your OCSP manual for additional information.

#### Note

- OCSP transports messages over HTTP, so there may be a time delay when you access the OCSP server.
- If the OCSP server depends on normal CRL processing to check revocation status, the same time delay that affects CRLs will also apply to OCSP.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>crypto pki trustpoint <em>name</em></td>
<td>Declares the trustpoint and a given name and enters ca-trustpoint config mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# crypto pki trustpoint</td>
<td></td>
</tr>
<tr>
<td>hazel</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>ocsp url <em>url</em></td>
<td>The <em>url</em> argument specifies the URL of an OCSP server so that the trustpoint can check the certificate status. This URL overrides the URL of the OCSP server (if one exists) in the Authority Info Access (AIA) extension of the certificate. All certificates associated with a configured trustpoint are checked by the OCSP server. The URL can be a hostname, IPv4 address, or an IPv6 address.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(ca-trustpoint)# ocsp url</td>
<td></td>
</tr>
<tr>
<td><a href="http://ocsp-server">http://ocsp-server</a></td>
<td></td>
</tr>
<tr>
<td>- or -</td>
<td></td>
</tr>
<tr>
<td>Device(ca-trustpoint)# ocsp url</td>
<td></td>
</tr>
<tr>
<td><a href="http://10.10.10.1:80">http://10.10.10.1:80</a></td>
<td></td>
</tr>
<tr>
<td>- or -</td>
<td></td>
</tr>
<tr>
<td>Device(ca-trustpoint)# ocsp url</td>
<td></td>
</tr>
<tr>
<td>http://[2001DB8:1:1::2]:80</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>revocation-check <em>method1</em> [method2<em>method3</em>]]</td>
<td>Checks the revocation status of a certificate.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(ca-trustpoint)# revocation-check</td>
<td></td>
</tr>
<tr>
<td>ocsp none</td>
<td></td>
</tr>
<tr>
<td>checks the revocation status of a certificate.</td>
<td></td>
</tr>
<tr>
<td>• crl — Certificate checking is performed by a CRL. This is the default option.</td>
<td></td>
</tr>
<tr>
<td>• none — Certificate checking is ignored.</td>
<td></td>
</tr>
<tr>
<td>• ocsp — Certificate checking is performed by an OCSP server.</td>
<td></td>
</tr>
<tr>
<td>If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>ocsp disable-nonce</td>
<td>(Optional) Specifies that a nonce, or an OCSP request unique identifier, will not be sent during peer communications with the OCSP server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(ca-trustpoint)# ocsp</td>
<td></td>
</tr>
<tr>
<td>disable-nonce</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Step 7</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(ca-trustpoint)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>(Optional) Displays information about your certificates.</td>
</tr>
<tr>
<td>show crypto pki certificates</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# show crypto pki certificates</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>Displays information about the trustpoint configured in router.</td>
</tr>
<tr>
<td>show crypto pki trustpoints [status</td>
<td>label</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# show crypto pki trustpoints</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Certificate Authorization and Revocation Settings**

Perform this task to specify a certificate-based ACL, to ignore revocation checks or expired certificates, to manually override the default CDP location, to manually override the OCSP server setting, to configure CRL caching, or to set session acceptance or rejection based on a certificate serial number, as appropriate.

**Configuring Certificate-Based ACLs to Ignore Revocation Checks**

To configure your router to use certificate-based ACLs to ignore revocation checks and expired certificates, perform the following steps:

- Identify an existing trustpoint or create a new trustpoint to be used when verifying the certificate of the peer. Authenticate the trustpoint if it has not already been authenticated. The router may enroll with this trustpoint if you want. Do not set optional CRLs for the trustpoint if you plan to use the `match certificate` command and `skip revocation-check` keyword.

- Determine the unique characteristics of the certificates that should not have their CRL checked and of the expired certificates that should be allowed.

- Define a certificate map to match the characteristics identified in the prior step.

- You can add the `match certificate` command and `skip revocation-check` keyword and the `match certificate command` and `allow expired-certificate` keyword to the trustpoint that was created or identified in the first step.
Certificate maps are checked even if the peer’s public key is cached. For example, when the public key is cached by the peer, and a certificate map is added to the trustpoint to ban a certificate, the certificate map is effective. This prevents a client with the banned certificate, which was once connected in the past, from reconnecting.

Manually Overriding CDPs in a Certificate

Users can override the CDPs in a certificate with a manually configured CDP. Manually overriding the CDPs in a certificate can be advantageous when a particular server is unavailable for an extended period of time. The certificate’s CDPs can be replaced with a URL or directory specification without reissuing all of the certificates that contain the original CDP.

Manually Overriding the OCSP Server Setting in a Certificate

Administrators can override the OCSP server setting specified in the Authority Information Access (AIA) field of the client certificate or set by the issuing the `ocsp url` command. One or more OCSP servers may be manually specified, either per client certificate or per group of client certificates by the `match certificate override ocsp` command. The `match certificate override ocsp` command overrides the client certificate AIA field or the `ocsp url` command setting if a client certificate is successfully matched to a certificate map during the revocation check.

Note

Only one OCSP server can be specified per client certificate.

Configuring CRL Cache Control

By default, a new CRL will be downloaded after the currently cached CRL expires. Administrators can either configure the maximum amount of time in minutes a CRL remains in the cache by issuing the `crl cache delete-after` command or disable CRL caching by issuing the `crl cache none` command. Only the `crl-cache delete-after` command or the `crl-cache none` command may be specified. If both commands are entered for a trustpoint, the last command executed will take effect and a message will be displayed.

Neither the `crl-cache none` command nor the `crl-cache delete-after` command affects the currently cached CRL. If you configure the `crl-cache none` command, all CRLs downloaded after this command is issued will not be cached. If you configure the `crl-cache delete-after` command, the configured lifetime will only affect CRLs downloaded after this command is issued.

This functionality is useful when a CA issues CRLs with no expiration date or with expiration dates days or weeks ahead.

Configuring Certificate Serial Number Session Control

A certificate serial number can be specified to allow a certificate validation request to be accepted or rejected by the trustpoint for a session. A session may be rejected, depending on certificate serial number session control, even if a certificate is still valid. Certificate serial number session control may be configured by using either a certificate map with the `serial-number` field or an AAA attribute, with the `cert-serial-not` command.

Using certificate maps for session control allows an administrator to specify a single certificate serial number. Using the AAA attribute allows an administrator to specify one or more certificate serial numbers for session control.
Before you begin

- The trustpoint should be defined and authenticated before attaching certificate maps to the trustpoint.
- The certificate map must be configured before the CDP override feature can be enabled or the `serial-number` command is issued.
- The PKI and AAA server integration must be successfully completed to use AAA attributes as described in “PKI and AAA Server Integration for Certificate Status.”

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
  * Example:
  
  ```
  Device> enable
  ```  |
| Step 2 | `configure terminal` | Enters global configuration mode.  
  * Example:
  
  ```
  Device# configure terminal
  ```  |
| Step 3 | `crypto pki certificate map label sequence-number` | Defines values in a certificate that should be matched or not matched and enters ca-certificate-map configuration mode.  
  * Example:
  
  ```
  Device(config)# crypto pki certificate map Group 10
  ```  |
| Step 4 | `field-name match-criteria match-value` | Specifies one or more certificate fields together with their matching criteria and the value to match.  
  * Example:
  
  ```
  Device(ca-certificate-map)# subject-name co MyExample
  ```  
  The *field-name* is one of the following case-insensitive name strings or a date:  
  - `alt-subject-name`
  - `expires-on`
  - `issuer-name`
  - `name`
  - `serial-number`
  - `subject-name`
  - `unstructured-subject-name`
  - `valid-start`
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Note**          | Date field format is dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss. The *match-criteria* is one of the following logical operators:  
  • *co* — contains (valid only for name fields and serial number field)  
  • *eq* — equal (valid for name, serial number, and date fields)  
  • *ge* — greater than or equal (valid only for date fields)  
  • *lt* — less than (valid only for date fields)  
  • *nc* — does not contain (valid only for name fields and serial number field)  
  • *ne* — not equal (valid for name, serial number, and date fields)  
  The *match-values* is the name or date to test with the logical operator assigned by match-criteria. **Note** Use this command only when setting up a certificate-based ACL—not when setting up a certificate-based ACL to ignore revocation checks or expired certificates. |
| **Step 5**        | exit Returns to global configuration mode. |
| **Example:**      | Device(ca-certificate-map)# exit |
| **Step 6**        | crypto pki trustpoint *name* Declares the trustpoint, given name and enters ca-trustpoint configuration mode. |
| **Example:**      | Device(config)# crypto pki trustpoint Access2 |
| **Step 7**        | Do one of the following:  
  • *crl-cache* none  
  • *crl-cache delete-after* time  
  (Optional) Disables CRL caching completely for all CRLs associated with the trustpoint.  
  The *crl-cache none* command does not affect any currently cached CRLs. All CRLs downloaded after this command is configured will not be cached. |
<p>| <strong>Example:</strong>      | Device(ca-trustpoint)# crl-cache none |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Device(ca-trustpoint)# crl-cache delete-after 20 | (Optional) Specifies the maximum time CRLs will remain in the cache for all CRLs associated with the trustpoint. 
  
  - **time** — The amount of time in minutes before the CRL is deleted. 

  The **crl-cache delete-after** command does not affect any currently cached CRLs. The configured lifetime will only affect CRLs downloaded after this command is configured. |

**Step 8**  
**match certificate**  
 certificate-map-label 
allow expired-certificate | skip revocation-check | skip authorization-check 

**Example:**  
Device(ca-trustpoint)# match certificate Group skip revocation-check 

((Optional) Associates the certificate-based ACL (that was defined via the **crypto pki certificate map** command) to a trustpoint.  

  - **certificate-map-label** — Must match the **label** argument specified via the **crypto pki certificate map** command. 
  
  - **allow expired-certificate** — Ignores expired certificates. 
  
  - **skip revocation-check** — Allows a trustpoint to enforce CRLs except for specific certificates. 
  
  - **skip authorization-check** — Skips the AAA check of a certificate when PKI integration with an AAA server is configured. |

**Step 9**  
**match certificate**  
 certificate-map-label 
override cdp | url | directory | string 

**Example:**  
Device(ca-trustpoint)# match certificate Group1 override cdp url http://server.cisco.com 

((Optional) Manually overrides the existing CDP entries for a certificate with a URL or directory specification.  

  - **certificate-map-label** — A user-specified label that must match the **label** argument specified in a previously defined **crypto pki certificate map** command. 
  
  - **url** — Specifies that the certificate’s CDPs will be overridden with an HTTP or LDAP URL. 
  
  - **directory** — Specifies that the certificate’s CDPs will be overridden with an LDAP directory specification. 
  
  - **string** — The URL or directory specification. |
Some applications may time out before all CDPs have been tried and will report an error message. The error message will not affect the router, and the Cisco IOS software will continue attempting to retrieve a CRL until all CDPs have been tried.

### Step 10

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>match certificate certificate-map-label override ocsp [trustpoint trustpoint-label] sequence-number url ocsp-url</td>
<td>(Optional) Specifies an OCSP server, either per client certificate or per group of client certificates, and may be issued more than once to specify additional OCSP servers and client certificate settings including alternative PKI hierarchies.</td>
</tr>
</tbody>
</table>

**Example:**

Device(ca-trustpoint)# match certificate mycertmapname override ocsp trustpoint mytp 15 url http://192.0.2.2

- **certificate-map-label** — The name of an existing certificate map.
- **trustpoint** — The trustpoint to be used when validating the OCSP server certificate.
- **sequence-number** — The order the `match certificate override ocsp` command statements apply to the certificate being verified. Matches are performed from the lowest sequence number to the highest sequence number. If more than one command is issued with the same sequence number, it overwrites the previous OCSP server override setting.
- **url** — The URL of the OCSP server.

When the certificate matches a configured certificate map, the AIA field of the client certificate and any previously issued `ocsp url` command settings are overwritten with the specified OCSP server.

If no map-based match occurs, one of the following two cases will continue to apply to the client certificate.

- If OCSP is specified as the revocation method, the AIA field value will continue to apply to the client certificate.
- If the `ocsp url` configuration exists, the `ocsp url` configuration settings will continue to apply to the client certificates.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(ca-trustpoint)# exit</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>aaa new-model</td>
<td>(Optional) Enables the AAA access control model.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>aaa attribute list list-name</td>
<td>(Optional) Defines an AAA attribute list locally on a router and enters config-attr-list configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# aaa attribute list crl</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>attribute type {name} {value}</td>
<td>(Optional) Defines an AAA attribute type that is to be added to an AAA attribute list locally on a router.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-attr-list)# attribute type cert-serial-not 6C4A</td>
<td>To configure certificate serial number session control, an administrator may specify a specific certificate in the value field to be accepted or rejected based on its serial number where name is set to cert-serial-not. If the serial number of the certificate matches the serial number specified by the attribute type setting, the certificate will be rejected. For a full list of available AAA attribute types, execute the show aaa attributes command.</td>
</tr>
<tr>
<td>15</td>
<td>exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(ca-trustpoint)# exit</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>exit</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# exit</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>show crypto pki certificates</td>
<td>(Optional) Displays the components of the certificates installed on the router if the CA certificate has been authenticated.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show crypto pki certificates</td>
<td></td>
</tr>
</tbody>
</table>
Example

The following is a sample certificate. The OCSP-related extensions are shown using exclamation points.

Certificate:

Data:

  Version: v3
  Serial Number: 0x14
  Signature Algorithm: SHAwithRSA - 1.2.840.113549.1.1.4
  Issuer: CN=CA server, OU=PKI, O=Cisco Systems

Validity:
  Not Before: Thursday, August 8, 2002 4:38:05 PM PST
  Not After: Tuesday, August 7, 2003 4:38:05 PM PST

Subject: CN=OCSP server, OU=PKI, O=Cisco Systems

Subject Public Key Info:
  Algorithm: RSA - 1.2.840.113549.1.1.1
  Public Key:
    Exponent: 65537
    Public Key Modulus: (2048 bits):
      <snip>

Extensions:
  Identifier: Subject Key Identifier - 2.5.29.14
    Critical: no
    Key Identifier:
      <snip>
  Identifier: Authority Key Identifier - 2.5.29.35
    Critical: no
    Key Identifier:
      <snip>

  Identifier: OCSP NoCheck: - 1.3.6.1.5.5.7.48.1.5
    Critical: no

  Identifier: Extended Key Usage: - 2.5.29.37
    Critical: no
    Extended Key Usage:
      OCSPSigning

  Identifier: CRL Distribution Points - 2.5.29.31
    Critical: no
    Number of Points: 1
    Point 0
      Distribution Point:
        [URIName: ldap://CA-server/CN=CA server, OU=PKI, O=Cisco Systems]

Signature:
  Algorithm: SHAwithRSA - 1.2.840.113549.1.1.4
  Signature:
    <snip>

The following example shows an excerpt of the running configuration output when adding a match certificate override ocsp command to the beginning of an existing sequence:

```
match certificate map3 override ocsp 5 url http://192.0.2.3/
signature
```

```
match certificate map1 override ocsp 10 url http://192.0.2.1/
match certificate map2 override ocsp 15 url http://192.0.2.2/
```
The following example shows an excerpt of the running configuration output when an existing `match certificate override ocsp` command is replaced and a trustpoint is specified to use an alternative PKI hierarchy:

```
match certificate map4 override ocsp trustpoint tp4 10 url http://192.0.2.4/newvalue
show running-configuration
match certificate map3 override ocsp trustpoint tp3 5 url http://192.0.2.3/
match certificate map1 override ocsp trustpoint tp1 10 url http://192.0.2.1/
match certificate map4 override ocsp trustpoint tp4 10 url http://192.0.2.4/newvalue
match certificate map2 override ocsp trustpoint tp2 15 url http://192.0.2.2/
```

**Troubleshooting Tips**

If you ignored revocation check or expired certificates, you should carefully check your configuration. Verify that the certificate map properly matches either the certificate or certificates that should be allowed or the AAA checks that should be skipped. In a controlled environment, try modifying the certificate map and determine what is not working as expected.

**Configuring Certificate Chain Validation**

Perform this task to configure the processing level for the certificate chain path of your peer certificates.

**Before you begin**

- The device must be enrolled in your PKI hierarchy.
- The appropriate key pair must be associated with the certificate.

**Note**

- A trustpoint associated with the root CA cannot be configured to be validated to the next level.

The `chain-validation` command is configured with the `continue` keyword for the trustpoint associated with the root CA, an error message will be displayed and the chain validation will revert to the default `chain-validation` command setting.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>crypto pki trustpointname</td>
<td>Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# crypto pki trustpoint ca-sub1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>chain-validation [{stop</td>
<td>continue} [parent-trustpoint]]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(ca-trustpoint)# chain-validation continue ca-sub1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Use the stop keyword to specify that the certificate is already trusted. This is the default setting.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Use the continue keyword to specify that the subordinate CA certificate associated with the trustpoint must be validated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The parent-trustpoint argument specifies the name of the parent trustpoint the certificate must be validated against.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>Returns to global configuration mode</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(ca-trustpoint)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Examples for Setting Up Authorization and Revocation of Certificates**

**Configuration and Verification Examples for PKI AAA Authorization**

This section provides configuration examples of PKI AAA authorizations:

**Example: Router Configuration**

The following `show running-config` command output shows the working configuration of a router that is set up to authorize VPN connections using the PKI Integration with AAA Server feature:

```
Device# show running-config
Building configuration...
!
version 12.3
!
hostname router7200router7200
!
aaa new-model
!
```
aaa authentication login default group tacacs+
aaa authentication login no_tacacs enable
aaa authentication ppp default group tacacs+
aaa authorization exec ACSLab group tacacs+
aaa accounting exec ACSLab start-stop group tacacs+
aaa accounting network default start-stop group ACSLab
aaa session-id common

ip domain name example.com

crypto pki trustpoint EM-CERT-SERV
enrollment url http://192.0.2.33:80
serial-number
rsakeypair STOREVPN 2048
auto-enroll
authorization list ACSLab

crypto pki certificate chain EM-CERT-SERV
certificate ca 01
quit
certificate 04
30820214 3082017D A0030201 02000104 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 454DD2D4 4552542D 53455256 301E170D 03043031
31393232 30323535 5A170D30 33503313 38323230 3235355A 3030312E 030E0063
55040513 03314437 45424434 301C0609 2A864886 F70D0109 02160F37 3230302D
312E6772 696C2E63 6F6D0801 9F300D06 029A8648 86F70D01 010050 0318100D
30819802 81810OBD F3B837AA 92DF5931 26BD4A14 9C2E0A31 5A7203C4 92F86DE8
7D2357A6 BCC8596F A38A9B10 47435626 D59A8F2A 123195BB B1AA5EA0
5CA162FF 8C3AA4AF 833E9F27 B0316B42 61B8AE18 40F2E3B4 F996BEFE 382C7283
3792A369 236F9561 8748AA3F BC41F012 B859BD9C DB4F75EE 33EEE289 704BAD6F
FD904403 0F555702 03010001 A3573055 30250603 551D1F04 1E301C30 1AA018A0
16691466 7474030A 2F2F3E53 2E323437 2E313037 2E393330 0B060355 1D0F0404
030205A0 301F0603 551D2304 18301680 1420F4CB CP01BC56 F5BD4C06 0A0D4E67
341A6E12 D1300D06 029A8648 86F70D01 010050 0318100D 79EF9018 FB955108
12F42A56 2A38384BC A4E222FE F0D6187F D5A56737 C0B214AC 0A9E75C3 7C4735F9
08DEEFF2 08B13A73 D79E0FA9 6D20CD2D 82798C8D 21CD30EC 3B2505A1 3897303C
15A605DA 8A13F06D 51043D37 E56E45DF A65F437D 4E836093 9687984D C45FD61D
EC1F160C 1ABC9D03 49FB11B1 D08ED6C 463E1090 F34C59E4
quit
certificate ca 01
30820207 30820170 A0030201 02000104 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 454DD2D4 4552542D 53455256 301E170D 03033132
31363231 34373432 5A170D30 03313231 35323134 3734325A 30173115 031D0603
55040313 0C454D2D 43455254 2D534552 5630819F 300D0609 2A864886 F70D0101
01050003 8180D003 81890281 8100C14D 833641CF D784F516 DAB65C0C 7BC3BC9C
589223A8 99A7DC14 047F4EF2 A4EEE8F5 E3BFAE97 F29F908F D889E6A1 2C726C69
54A29870 7E7363FF 3CD1F991 F5A37CFF 3FDD3DD0 9E486C44 A2E34595 C2D078BB
E9DE981E B733B688 AA8916CO A8048607 D34B3C03 64BDC011 161FC103 13C06500
22D66E75 7BC0333 7F1B151F 32830203 010001A3 63306130 0F603055 1D301011
FF040530 030101FF 300E0603 551D0F01 01FF0404 30020186 301D0603 551D0E04
16041420 F4BCBF01 C56F5BD 4C060A0F 4E67341A E612D130 1F060355 1D30418
30166014 20PC4BCBF 081565F5 BD4C060A FD4E6734 1AE612D1 300D0609 2A864886
F70D0101 04050003 81810085 D2386F45 4107116B AD3C909 CBE84630 5FB2A6B5
B5D52062 528E920E 02F303AE 180F2F2E A44C06ED 0F59F18D 7B50264F 30442C41
0A0F9C4E 70853CB5 0ADD8DE8 88E636BD 24110DF4 DB62AE58 3879A93E 12A0FB1C 2E27CC27 EC741EFC AEE2F5CF CA80B427 615A88D5 6D6EDC3 7F9C2C79
3963E363 F2989FB9 795BA8
quit

crypto isakmp policy 10
encr aes
group 14
crypto ipsec transform-set ISC_TS_1 esp-aes esp-sha-hmac
  
crypto ipsec profile ISC_IPSEC_PROFILE_2
  set security-association lifetime kilobytes 530000000
  set security-association lifetime seconds 14400
  set transform-set ISC_TS_1
  
interface Tunnel0
  description MGRE Interface provisioned by ISC
  bandwidth 10000
  ip address 192.0.2.172 255.255.255.0
  no ip redirects
  ip mtu 1408
  ip nhrp map multicast dynamic
  ip nhrp network-id 101
  ip nhrp holdtime 500
  ip nhrp server-only
  no ip split-horizon eigrp 101
  tunnel source FastEthernet2/1
  tunnel mode gre multipoint
  tunnel key 101
  tunnel protection ipsec profile ISC_IPSEC_PROFILE_2
  
interface FastEthernet2/0
  ip address 192.0.2.1 255.255.255.0
  duplex auto
  speed auto
  
interface FastEthernet2/1
  ip address 192.0.2.2 255.255.255.0
  duplex auto
  speed auto
  
tacacs-server host 192.0.2.55 single-connection
  tacacs-server directed-request
  tacacs-server key company lab
  
ntp master 1
  
end

Example: Debug of a Successful PKI AAA Authorization

The following `show debugging` command output shows a successful authorization using the PKI Integration with AAA Server feature:

```
Device# show debugging

General OS:
  TACACS access control debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
Cryptographic Subsystem:
  Crypto PKI Trans debugging is on
Device#
May 28 19:36:11.117: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
```
Example: Debug of a Failed PKI AAA Authorization

The following show debugging command output shows that the router is not authorized to connect using VPN. The messages are typical of those that you might see in such a situation.

In this example, the peer username was configured as not authorized, by moving the username to a Cisco Secure ACS group called VPN_Router_Disabled in Cisco Secure ACS. The router, router7200.example.com, has been configured to check with a Cisco Secure ACS AAA server prior to establishing a VPN connection to any peer.

show crypto isakmp sa

dst     src     state     conn-id slot
192.0.2.22 192.0.2.102 QM_IDLE    84   0

Example: Debug of a Failed PKI AAA Authorization

Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches)
Examples: Configuring a Revocation Mechanism

This section contains the following configuration examples that can be used when specifying a revocation mechanism for your PKI:

Example: Configuring an OCSP Server

The following example shows how to configure the router to use the OCSP server that is specified in the AIA extension of the certificate:
Example: Specifying a CRL and Then an OCSP Server

The following example shows how to configure the router to download the CRL from the CDP. If the CRL is unavailable, the OCSP server that is specified in the AIA extension of the certificate will be used. If both options fail, certificate verification will also fail.

Example: Specifying an OCSP Server

The following example shows how to configure your router to use the OCSP server at the HTTP URL “http://myocspserver:81.” If the server is down, the revocation check will be ignored.

Example: Disabling Nonces in Communications with the OCSP Server

The following example shows communications when a nonce, or a unique identifier for the OCSP request, is disabled for communications with the OCSP server:

Example: Configuring a Hub Router at a Central Site for Certificate Revocation Checks

The following example shows a hub router at a central site that is providing connectivity for several branch offices to the central site.

The branch offices are also able to communicate directly with each other using additional IPSec tunnels between the branch offices.

The CA publishes CRLs on an HTTP server at the central site. The central site checks CRLs for each peer when setting up an IPSec tunnel with that peer.

The example does not show the IPSec configuration--only the PKI-related configuration is shown.

Home Office Hub Configuration

crypto pki trustpoint VPN-GW
enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
serial-number none
fqdn none
ip-address none
subject-name o=Home Office Inc,cn=Central VPN Gateway
revocation-check crl
Central Site Hub Router

Device# show crypto ca certificate
Certificate
Status: Available
Certificate Serial Number: 2F62BE14000000000CA0
Certificate Usage: General Purpose
Issuer:
cn=Central Certificate Authority
o=Home Office Inc
Subject:
Name: Central VPN Gateway
cn=Central VPN Gateway
o=Home Office Inc
CRL Distribution Points:
http://ca.home-office.com/CertEnroll/home-office.crl
Validity Date:
start date: 00:43:26 GMT Sep 26 2003
end date: 00:53:26 GMT Sep 26 2004
renew date: 00:00:00 GMT Jan 1 1970
Associated Trustpoints: VPN-GW

Certificate
Status: Available
Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
Certificate Usage: Signature
Issuer:
cn=Central Certificate Authority
o=Home Office Inc
Subject:
cn=Central Certificate Authority
o=Home Office Inc
CRL Distribution Points:
http://ca.home-office.com/CertEnroll/home-office.crl
Validity Date:
start date: 22:19:29 GMT Oct 31 2002
end date: 22:27:27 GMT Oct 31 2017
Associated Trustpoints: VPN-GW

Trustpoint on the Branch Office Router

crypto pki trustpoint home-office
enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
serial-number none
fqdn none
ip-address none
subject-name o=Home Office Inc,cn=Branch 1
revocation-check crl

A certificate map is entered on the branch office router.

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
branch1(config)# crypto pki certificate map central-site 10
branch1(ca-certificate-map)#

The output from the show certificate command on the central site hub router shows that the certificate was issued by the following:

cn=Central Certificate Authority
o=Home Office Inc
These two lines are combined into one line using a comma (,) to separate them, and the original lines are added as the first criteria for a match.

Device(ca-certificate-map)# issuer-name co cn=Central Certificate Authority, ou=Home Office Inc

The above line wrapped but should be shown on one line with the line above it.

The same combination is done for the subject name from the certificate on the central site router (note that the line that begins with “Name:” is not part of the subject name and must be ignored when creating the certificate map criteria). This is the subject name to be used in the certificate map.

cn=Central VPN Gateway
o=Home Office Inc

Device(ca-certificate-map)# subject-name eq cn=central vpn gateway, o=home office inc

Now the certificate map is added to the trustpoint that was configured earlier.

Device(ca-certificate-map)# crypto pki trustpoint home-office
Device(ca-trustpoint)# match certificate central-site skip revocation-check
Device(config)# exit

The configuration is checked (most of configuration is not shown).

Device# write term

crypto pki trustpoint home-office
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc,cn=Branch 1
  revocation-check crl
  match certificate central-site skip revocation-check

crypto pki certificate map central-site 10
  issuer-name co cn=Central Certificate Authority, ou=Home Office Inc
  subject-name eq cn=central vpn gateway, o=home office inc

Note that the issuer-name and subject-name lines have been reformatted to make them consistent for later matching with the certificate of the peer.

If the branch office is checking the AAA, the trustpoint will have lines similar to the following:

crypto pki trustpoint home-office
  auth list allow_list
  auth user subj commonname

After the certificate map has been defined as was done above, the following command is added to the trustpoint to skip AAA checking for the central site hub.

match certificate central-site skip authorization-check
In both cases, the branch site router has to establish an IPSec tunnel to the central site to check CRLs or to contact the AAA server. However, without the match certificate command and central-site skip authorization-check (argument and keyword), the branch office cannot establish the tunnel until it has checked the CRL or the AAA server. (The tunnel will not be established unless the match certificate command and central-site skip authorization-check argument and keyword are used.)

The match certificate command and allow expired-certificate keyword would be used at the central site if the router at a branch site had an expired certificate and it had to establish a tunnel to the central site to renew its certificate.

**Trustpoint on the Central Site Router**

```plaintext
crypto pki trustpoint VPN-GW
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc,cn=Central VPN Gateway
  revocation-check crl
```

**Trustpoint on the Branch 1 Site Router**

```
Device# show crypto ca certificate
Certificate
  Status: Available
  Certificate Serial Number: 2F62BE1400000000CA0
  Certificate Usage: General Purpose
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    Name: Branch 1 Site
    cn=Branch 1 Site
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 00:43:26 GMT Sep 26 2003
    end date: 00:53:26 GMT Oct 3 2003
    renew date: 00:00:00 GMT Jan 1 1970
  Associated Trustpoints: home-office

CA Certificate
  Status: Available
  Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
  Certificate Usage: Signature
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    cn=Central Certificate Authority
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 22:19:29 GMT Oct 31 2002
    end date: 22:27:27 GMT Oct 31 2017
  Associated Trustpoints: home-office
```

A certificate map is entered on the central site router.
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# crypto pki certificate map branch1 10
Device(config)# issuer-name co cn=Central Certificate Authority, ou=Home Office Inc
The above line wrapped but should be part of the line above it.
Device(config)# subject-name eq cn=Branch 1 Site, o=home office inc

The certificate map is added to the trustpoint.

Device(config)# crypto pki trustpoint VPN-GW
Device(config)# match certificate branch1 allow expired-certificate
Device(config)# exit
Router (config) #

The configuration should be checked (most of the configuration is not shown).

Device# write term

Examples: Configuring Certificate Authorization and Revocation Settings

This section contains the following configuration examples that can be used when specifying a CRL cache control setting or certificate serial number session control:

Configuring CRL Cache Control

The following example shows how to disable CRL caching for all CRLs associated with the CA1 trustpoint:

crypto pki trustpoint CA1
  enrollment url http://CA1:80
  ip-address FastEthernet0/0
  crl query ldap://ldap CA1
  revocation-check crl
  crl-cache none

The current CRL is still cached immediately after executing the example configuration shown above:

Device# show crypto pki crls

CRL Issuer Name:
  cn-name Cert Manager, ou=pki, o=example.com, c=US
Configuring Certificate Serial Number Session Control

When the current CRL expires, a new CRL is then downloaded to the router at the next update. The `crl-cache none` command takes effect and all CRLs for the trustpoint are no longer cached; caching is disabled. You can verify that no CRL is cached by executing the `show crypto pki crls` command. No output will be shown because there are no CRLs cached.

The following example shows how to configure the maximum lifetime of 2 minutes for all CRLs associated with the CA1 trustpoint:

```plaintext
crypto pki trustpoint CA1
    enrollment url http://CA1:80
    ip-address FastEthernet0/0
    crl query ldap://ldap_CA1
    revocation-check crl
    crl-cache delete-after 2
```

The current CRL is still cached immediately after executing the example configuration above for setting the maximum lifetime of a CRL:

Device# show crypto pki crls

CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=example.com,c=US
    LastUpdate: 18:57:42 GMT Nov 26 2005
    NextUpdate: 22:57:42 GMT Nov 26 2005
    Retrieved from CRL Distribution Point:
        ldap://ldap.example.com/CN=name Cert Manager,O=example.com

When the current CRL expires, a new CRL is downloaded to the router at the next update and the `crl-cache delete-after` command takes effect. This newly cached CRL and all subsequent CRLs will be deleted after a maximum lifetime of 2 minutes.

You can verify that the CRL will be cached for 2 minutes by executing the `show crypto pki crls` command. Note that the NextUpdate time is 2 minutes after the LastUpdate time.

Device# show crypto pki crls

CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=example.com,c=US
    LastUpdate: 22:57:42 GMT Nov 26 2005
    NextUpdate: 22:59:42 GMT Nov 26 2005
    Retrieved from CRL Distribution Point:
        ldap://ldap.example.com/CN=name Cert Manager,O=example.com

Configuring Certificate Serial Number Session Control

The following example shows the configuration of certificate serial number session control using a certificate map for the CA1 trustpoint:

```plaintext
crypto pki trustpoint CA1
    enrollment url http://CA1
    chain-validation stop
    crl query ldap://ldap_server
    revocation-check crl
    match certificate crl
```
crypto pki certificate map crl 10
  serial-number co 279d

If the *match-criteria* value is set to *eq* (equal) instead of *co* (contains), the serial number must match the certificate map serial number exactly, including any spaces.

The following example shows the configuration of certificate serial number session control using AAA attributes. In this case, all valid certificates will be accepted if the certificate does not have the serial number “4ACA.”

```plaintext
crypto pki trustpoint CA1
  enrollment url http://CA1
  ip-address FastEthernet0/0
  crl query ldap://ldap_CA1
  revocation-check crl
  aaa new-model
  aaa attribute list crl
    attribute-type aaa-cert-serial-not 4ACA
```

The server log shows that the certificate with the serial number “4ACA” was rejected. The certificate rejection is shown using exclamation points.

```
Dec 3 04:24:39.051: CRYPTO_PKI: Trust-Point CA1 picked up
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.051: CRYPTO_PKI: unlocked trustpoint CA1, refcount is 0
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.135: CRYPTO_PKI: validation path has 1 certs
Dec 3 04:24:39.135: CRYPTO_PKI: Found a issuer match
Dec 3 04:24:39.135: CRYPTO_PKI: Using CA1 to validate certificate
Dec 3 04:24:39.135: CRYPTO_PKI: Anticipate checking AAA list:'CRL'
Dec 3 04:24:39.135: CRYPTO_PKI: AAA: checking AAA authorization (CRL, PKIAAA-L1, <all>)
Dec 3 04:24:39.135: CRYPTO_PKI: pre-authorization chain validation status (0x4)
Dec 3 04:24:39.135: AAA/AUTHOR (0x21): Pick method list 'CRL'

Dec 3 04:24:39.175: CRYPTO_PKI: AAA: reply attribute ("cert-application" = "all")
Dec 3 04:24:39.175: CRYPTO_PKI: AAA: reply attribute ("cert-trustpoint" = "CA1")
Dec 3 04:24:39.175: CRYPTO_PKI: AAA: reply attribute ("cert-serial-not" = "4ACA")
Dec 3 04:24:39.175: CRYPTO_PKI: AAA: cert-serial doesn't match ("4ACA" != "4ACA")
Dec 3 04:24:39.175: CRYPTO_PKI: AAA: post-authorization chain validation status (0x7)
Dec 3 04:24:39.175: CRYPTO_PKI: chain cert was anchored to trustpoint CA1, and chain validation result was: CRYPTO_PKI_CERT_NOT_AUTHORIZED
Dec 3 04:24:39.175: %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from 192.0.2.43 is bad: certificate invalid
Dec 3 04:24:39.175: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main mode failed with peer protocol
```
Examples: Configuring Certificate Chain Validation

This section contains the following configuration examples that can be used to specify the level of certificate chain processing for your device certificates:

Configuring Certificate Chain Validation from Peer to Root CA

In the following configuration example, all of the certificates will be validated--the peer, SubCA11, SubCA1, and RootCA certificates.

```plaintext
crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none
  rsakeypair RootCA

crypto pki trustpoint SubCA1
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
  rsakeypair SubCA1

crypto pki trustpoint SubCA11
  enrollment terminal
  chain-validation continue SubCA1
  revocation-check none
  rsakeypair SubCA11
```

Configuring Certificate Chain Validation from Peer to Subordinate CA

In the following configuration example, the following certificates will be validated--the peer and SubCA1 certificates.

```plaintext
crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none
  rsakeypair RootCA

crypto pki trustpoint SubCA1
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
  rsakeypair SubCA1

crypto pki trustpoint SubCA11
  enrollment terminal
  chain-validation continue SubCA1
  revocation-check none
  rsakeypair SubCA11
```

Configuring Certificate Chain Validation Through a Gap

In the following configuration example, SubCA1 is not in the configured Cisco IOS hierarchy but is expected to have been supplied in the certificate chain presented by the peer.

If the peer supplies the SubCA1 certificate in the presented certificate chain, the following certificates will be validated--the peer, SubCA11, and SubCA1 certificates.
If the peer does not supply the SubCA1 certificate in the presented certificate chain, the chain validation will fail.

crypto pki trustpoint RootCA
   enrollment terminal
   chain-validation stop
   revocation-check none
   rsakeypair RootCA

crypto pki trustpoint SubCA1
   enrollment terminal
   chain-validation continue RootCA
   revocation-check none
   rsakeypair SubCA1

Additional References

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of PKI, including RSA keys, certificate enrollment, and CAs</td>
<td>“Cisco IOS PKI Overview: Understanding and Planning a PKI” module</td>
</tr>
<tr>
<td>RSA key generation and deployment</td>
<td>“Deploying RSA Keys Within a PKI” module</td>
</tr>
<tr>
<td>Certificate enrollment: supported methods, enrollment profiles, configuration tasks</td>
<td>“Configuring Certificate Enrollment for a PKI” module</td>
</tr>
<tr>
<td>Cisco IOS certificate server overview information and configuration tasks</td>
<td>“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment ” module</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="https://www.cisco.com/cisco/web/support/index.html">https://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Feature Information for Certificate Authorization and Revocation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 76: Feature Information for PKI Certificate Authorization and Revocation

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKI Certificate Authorization and Revocation</td>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>The feature was introduced.</td>
</tr>
</tbody>
</table>
## Secure Operation in FIPS Mode

- FIPS 140-2 Overview, on page 587
- Configure FIPS 140-2, on page 588
- Key Zeroization, on page 588
- Disable FIPS Mode, on page 589
- Verify FIPS Configuration, on page 589
- Additional References for Secure Operation in FIPS Mode, on page 590

### FIPS 140-2 Overview

The Federal Information Processing Standards (FIPS) Publication 140-2 (Security Requirements for Cryptographic Modules) details the U.S. and Canadian governments' requirements for cryptographic modules. FIPS 140-2 specifies certain cryptographic algorithms as secure, and it also identifies which algorithms should be used if a cryptographic module is to be called FIPS compliant. For more information on the FIPS 140-2 standard and validation program, refer to the National Institute of Standards and Technology (NIST) website.

The FIPS 140-2 Compliance Review (CR) documents for Cisco Catalyst series switches are posted on the following website:


Click the link in the "Certification Date" column to view the CR Certificate.

Security Policy document describes the FIPS implementation, hardware installation, firmware initialization, and software configuration procedures for FIPS operation. You can access the FIPS 140-2 Consolidated Validation Certificate and Security Policy document on NIST Computer Security Resource Center. This website opens a Search window. In the Vendor field, enter "Cisco" and click Search. The resulting window provides a list of Cisco platforms that are FIPS Compliant. From the list, click the desired platform to obtain its Security Policy and Consolidated Certificate.

**Important**

This document describes FIPS mode behavior for Cisco Catalyst Switches in general. For more information on platform-specific FIPS 140-2 implementation, refer to the FIPS 14-2 Security Policy document for the platform.
Configure FIPS 140-2

Following is a generic procedure to enable FIPS mode of operation for Cisco Catalyst Switches. For a detailed configuration procedure, refer FIPS 140-2 Security Policy document for the required device.

**Procedure**

**Step 1**
(Optional) Enable FIPS 140-2 logging.

**Example:**
Device(config)# logging console errors

**Step 2**
Configure Authorization key.

**Example:**
Device(config)# fips authorization-key key
Note that key is 128 bits, which is, 16 HEX byte key.

**What to do next**
After you enable FIPS, reboot the system to start operating in FIPS mode.

**Key Zeroization**

A critical FIPS requirement is the capability to zeroize keys and passwords in the event of unsafe state triggers during FIPS mode of operation.

You can delete the FIPS authorization keys using the `no fips authorization-key` command in global configuration mode. This command deletes the key from flash. A reboot takes the system out of FIPS mode of operation.

If there is a security breach, use the `fips zeroize` command to delete all data including the running configuration, Trust Anchor Module, FIPS authorization keys, all ISE Server certificates, and IOS image in flash.

The system reboots after this command is executed.

**Caution**
FIPS zeroization is a critical step where all data is lost. Use it with caution.

Session keys are zeroized by the protocols programatically.

Device(config)# fips zeroize

**Critical Warning** - This command is irreversible and will zeroize the FVPK by Deleting the IOS image and config files, please use extreme caution and confirm with Yes on each of three iterations to complete. The system will reboot.
after the command executes successfully
Proceed ?? (yes/[no]):

Disable FIPS Mode

You can disable FIPS mode using the no fips authorization-key command.
The no fips authorization-key command deletes the authorization key from flash. Note that the authorization key is operational until you reload the switch.

To completely remove the authorization key and disable FIPS mode, reload the switch.

Device> enable
Device# config terminal
Device(config)# no fips authorization-key
Device(config)# end

Verify FIPS Configuration

Use the show fips status command to display the FIPS configuration information.

Use the show fips authorization-key command to display the hashed FIPS key.

Note

FIPS configuration information does not appear when you list the active configuration using the show running-config command or when you list the startup configuration using the show startup-config command.

The following are sample outputs of the show commands:

Device# show fips authorization-key
FIPS: Stored key (16) : 11111111111111111111111111111111

Device# show romvar
ROMMON variables:
PS1="switch: "
BOARDID="24666"
SWITCH_NUMBER="1"
TERMLINES="0"
MOTHERBOARD_ASSEMBLY_NUM="73-18506-02"
MOTHERBOARD_REVISION_NUM="04"
MODEL_REVISION_NUM="P2A"
POE1_ASSEMBLY_NUM="73-16123-03"
POE1_REVISION_NUM="A0"
POE1_SERIAL_NUM="F0C21335EF2"
POE2_ASSEMBLY_NUM="73-16123-03"
POE2_REVISION_NUM="A0"
POE2_SERIAL_NUM="F0C21335EF3"
IMAGE_UPGRADE="no"
MAC_ADDR="F8:7B:20:77:F7:80"
MODEL_NUM="C9300-48UN"
MOTHERBOARD_SERIAL_NUM="F0C21351BC3"
Additional References for Secure Operation in FIPS Mode

Standards and RFCs

<table>
<thead>
<tr>
<th>Standards/RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS 140-2</td>
<td>Security Requirements for Cryptographic Modules</td>
</tr>
</tbody>
</table>
**Technical Assistance**

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