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

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice. In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

© 2014–2020 Cisco Systems, Inc. All rights reserved.
CONTENTS

PREFACE

Preface xvii
  Audience xvii
  Document Conventions xvii
  Documentation Feedback xviii
  Communications, Services, and Additional Information xviii

CHAPTER 1

New and Changed Information 1

Overview 3

CHAPTER 2

Overview 3
  Authentication, Authorization, and Accounting 3
  RADIUS and TACACS+ Security Protocols 4
  SSH and Telnet 4
  IP ACLs 4

CHAPTER 3

Configuring Authentication, Authorization, and Accounting 5
  Information About AAA 5
  AAA Security Services 5
  Benefits of Using AAA 6
  Remote AAA Services 6
  AAA Server Groups 6
  AAA Service Configuration Options 6
  Authentication and Authorization Process for User Logins 7
  Prerequisites for Remote AAA 9
  Guidelines and Limitations for AAA 9
  Default AAA Settings 9
Configuring AAA 10
  Configuring Console Login Authentication Methods 10
  Configuring Default Login Authentication Methods 11
  Enabling Login Authentication Failure Messages 12
  Configuring Console Authorization Commands 12
  Enabling MSCHAP Authentication 13
  Configuring AAA Accounting Default Methods 14
Using AAA Server VSAs 15
  VSAs 15
  VSA Format 16
  Specifying Switch User Roles and SNMPv3 Parameters on AAA Servers 16
Secure Login Enhancements 16
  Configuring Login Parameters 17
  Configuration Examples for Login Parameters 18
  Configuring Login Block Per User 18
  Configuration Examples for Login Block Per User 19
  Restricting Sessions Per User—Per User Per Login 20
  Configuring Passphrase Length 20
  Configuring Passphrase Time Values 21
Locked User Accounts 24
  Logging Invalid Usernames 24
Changing Password 25
  Enabling the Password Prompt for User Name 26
  Support over SHA-256 Algorithm for Verifying OS Integrity 26
  Configuring Share Key Value for using RADIUS/TACACS+ 27
Monitoring and Clearing the Local AAA Accounting Log 27
Verifying the AAA Configuration 28
Configuration Examples for AAA 28

CHAPTER 4

Configuring RADIUS 29
  Information About RADIUS 29
  RADIUS Network Environments 29
  Information About RADIUS Operations 30
  RADIUS Server Monitoring 30
## Configuring TACACS+ Server Hosts

51

## Configuring TACACS+ Global Preshared Keys

52

## Configuring TACACS+ Server Preshared Keys

53

## Configuring TACACS+ Server Groups

53

## Configuring the Global Source Interface for TACACS+ Server Groups

55

## Specifying a TACACS+ Server at Login

55

## Configuring the Global TACACS+ Timeout Interval

56

## Configuring the Timeout Interval for a Server

56

## Configuring TCP Ports

57

## Configuring Periodic TACACS+ Server Monitoring

57

## Configuring the Dead-Time Interval

58

## Configuring ASCII Authentication

59

## Manually Monitoring TACACS+ Servers or Groups

60

## Disabling TACACS+

60

## Displaying TACACS+ Statistics

60

## Verifying the TACACS+ Configuration

61

## Configuration Examples for TACACS+

61

---

### CHAPTER 6

**Configuring SSH and Telnet**

63

## Information About SSH and Telnet

63

- **SSH Server**
- **SSH Client**
- **SSH Server Keys**
- **Telnet Server**

## Guidelines and Limitations for SSH

64

## Default Settings for SSH

64

## Configuring SSH

65

- **Generating SSH Server Keys**
- **Specifying the SSH Public Keys for User Accounts**
  - Specifying the SSH Public Keys in Open SSH Format
  - Specifying the SSH Public Keys in IETF SECSH Format
  - Specifying the SSH Public Keys in PEM-Formatted Public Key Certificate Form

## Starting SSH Sessions to Remote Devices

68

## Clearing SSH Hosts

68
CHAPTER 7

Configuring 802.1X 73

Information About 802.1X 73

Device Roles 73

Authentication Initiation and Message Exchange 75

Authenticator PAE Status for Interfaces 76

Ports in Authorized and Unauthorized States 76

MAC Authentication Bypass 77

80.1X and Port Security 78

Dynamic VLAN Assignment based on MAC-Based Authentication (MAB) 78

VLAN Assignment from RADIUS 79

Single Host and Multiple Hosts Support 79

Supported Topologies 79

Licensing Requirements for 802.1X 80

Prerequisites for 802.1X 80

80.1X Guidelines and Limitations 80

Default Settings for 802.1X 81

Configuring 802.1X 82

Process for Configuring 802.1X 82

Enabling the 80.1X Feature 82

Configuring AAA Authentication Methods for 80.1X 83

Controlling 80.1X Authentication on an Interface 84

Configuring 80.1X Authentication on Member Ports 85

Creating or Removing an Authenticator PAE on an Interface 87
## Changing the SXP Reconcile Period

141

## Changing the SXP Retry Period

141

## Verifying the Cisco TrustSec Configuration

142

## Configuration Examples for Cisco TrustSec

143

- **Example: Enabling Cisco TrustSec** 143
- **Example: Configuring AAA for Cisco TrustSec on a Seed Cisco NX-OS Device** 143
- **Example: Enabling Cisco TrustSec Authentication on an Interface** 144
- **Example: Configuring Cisco TrustSec Authentication in Manual Mode** 144
- **Example: Configuring Cisco TrustSec Role-Based Policy Enforcement for the Default VRF Instance** 144
- **Example: Configuring Cisco TrustSec Role-Based Policy Enforcement for a Nondefault VRF** 144
- **Example: Configuring Cisco TrustSec Role-Based Policy Enforcement for a VLAN** 145
- **Example: Configuring IPv4 Address to SGACL SGT Mapping for the Default VRF Instance** 145
- **Example: Configuring IPv4 Address to SGACL SGT Mapping for a Nondefault VRF Instance** 145
- **Example: Configuring IPv4 Address to SGACL SGT Mapping for a VLAN** 145
- **Example: Manually Configuring Cisco TrustSec SGACLs** 145
- **Example: Manually Configuring SXP Peer Connections** 146

## Additional References for Cisco TrustSec

146

## Feature History for Cisco TrustSec

147

---

### CHAPTER 9

**Configuring Access Control Lists** 149

- **Information About ACLs** 149
  - **IP ACL Types and Applications** 149
    - **Application Order** 150
  - **Rules** 151
    - **Source and Destination** 151
    - **Protocols** 151
    - **Implicit Rules** 151
    - **Additional Filtering Options** 152
    - **Sequence Numbers** 152
    - **Logical Operators and Logical Operation Units** 153
  - **Policy-Based ACLs** 153
  - **ACL Resource Management** 154
  - **Statistics and ACLs** 155
Minimum DHCP Snooping Configuration 209
Enabling or Disabling the DHCP Snooping Feature 209
Enabling or Disabling DHCP Snooping Globally 210
Enabling or Disabling DHCP Snooping on a VLAN 211
Enabling or Disabling Option 82 Data Insertion and Removal 212
Enabling or Disabling Strict DHCP Packet Validation 212
Configuring an Interface as Trusted or Untrusted 213
Enabling or Disabling the DHCP Relay Agent 214
Enabling or Disabling Option 82 for the DHCP Relay Agent 215
Enabling or Disabling VRF Support for the DHCP Relay Agent 216
Enabling or Disabling Subnet Broadcast Support for the DHCP Relay Agent on a Layer 3 Interface 217
Creating a DHCP Static Binding 218
Configuring the DHCPv6 Relay Agent 219
   Enabling or Disabling the DHCPv6 Relay Agent 219
   Enabling or Disabling VRF Support for the DHCPv6 Relay Agent 220
   Configuring the DHCPv6 Relay Source Interface 221
Configuring Lightweight DHCPv6 Relay Agent 222
   Configuring Lightweight DHCPv6 Relay Agent for an Interface 222
   Configuring Lightweight DHCPv6 Relay Agent for a VLAN 223
Verifying the DHCP Snooping Configuration 224
Displaying DHCP Bindings 224
Displaying and Clearing LDRA Information 225
Clearing the DHCP Snooping Binding Database 225
Clearing DHCP Relay Statistics 226
Clearing DHCPv6 Relay Statistics 226
Monitoring DHCP 226
Configuration Examples for DHCP Snooping 226
Configuration Examples for LDRA 227

CHAPTER 12

Configuring Control Plane Policing 229
   Information About CoPP 229
   Control Plane Protection 230
   Control Plane Packet Types 230
Classification for CoPP 231
Rate Controlling Mechanisms 231
CoPP Extended Rate 231
CoPP Class Maps 231
CoPP Policy Templates 234
Default CoPP Policy 234
Scaled Layer 2 CoPP Policy 236
Scaled Layer 3 CoPP Policy 237
Customizable CoPP Policy 238
CoPP and the Management Interface 239
Licensing Requirements for CoPP 239
Guidelines and Limitations for CoPP 239
Default Settings for CoPP 240
Configuring CoPP 241
Applying a CoPP Policy to the Switch 241
Modifying the Customized CoPP Policy 241
Configuring CoPP Extended Rate 242
Verifying the CoPP Configuration 243
Displaying the CoPP Configuration Status 243
Monitoring CoPP 244
Clearing the CoPP Statistics 245
Additional References for CoPP 245

CHAPTER 13
Configuring TCAM Carving 247
Information About TCAM Carving 247
Information About User-Defined Templates 247
Creating a User-Defined Template 250
Modifying a User Defined Template 251
Committing a User-Defined Template 251
Deleting a Template 252
Verifying the TCAM Carving Configuration 253

CHAPTER 14
Configuring Sup-region TCAM Monitoring 255
Information About Sup-region TCAM Monitoring 255
On-demand Detection of Corrupted Sup-region TCAM Entries 255
Periodic Detection of Corrupted Sup-region TCAM Entries 255
In-Service Software Upgrades and In-Service Software Downgrades 256
Licensing Requirements for Sup-region TCAM Monitoring 256
Guidelines and Limitations for Sup-region TCAM Monitoring 256
Default Setting for Sup-region TCAM Monitoring 256
Configuring Sup-region TCAM Monitoring 257
  Configuring On-Demand Detection of Corrupted Sup-region TCAM Entries 257
  Configuring Periodic Detection of Corrupted Sup-region TCAM Entries 257
  Correcting the Corrupted Sup-region TCAM Entries 258
Verifying Sup-region TCAM Monitoring 260
Configuration Examples for Sup-region TCAM Monitoring 260
Additional References for Sup-region TCAM Monitoring 260
Feature History for Sup-region TCAM Monitoring 261
Preface

The preface contains the following sections:

- Audience, on page xvii
- Document Conventions, on page xvii
- Documentation Feedback, on page xviii
- Communications, Services, and Additional Information, on page xviii

Audience

This publication is for network administrators who configure and maintain Cisco Nexus devices.

Document Conventions

As part of our constant endeavor to remodel our documents to meet our customers' requirements, we have modified the manner in which we document configuration tasks. As a result of this, you may find a deviation in the style used to describe these tasks, with the newly included sections of the document following the new format.

Command descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>Bold text indicates the commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Italic text indicates arguments for which the user supplies the values.</td>
</tr>
<tr>
<td>[x]</td>
<td>Square brackets enclose an optional element (keyword or argument).</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
<tr>
<td>variable</td>
<td>Indicates a variable for which you supply values, in context where italics cannot be used.</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
</tbody>
</table>

Examples use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screen font</td>
<td>Terminal sessions and information the switch displays are in screen font.</td>
</tr>
<tr>
<td>boldface screen font</td>
<td>Information you must enter is in boldface screen font.</td>
</tr>
<tr>
<td>italic screen font</td>
<td>Arguments for which you supply values are in italic screen font.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters, such as passwords, are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

This document uses the following conventions:

**Note**

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

**Caution**

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

---

**Documentation Feedback**

To provide technical feedback on this document, or to report an error or omission, please send your comments to:

We appreciate your feedback.

**Communications, Services, and Additional Information**

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](https://www.cisco.com/c/en/us/products/switches/nexus-6000-series nx-os chípnikl1z.html).
• To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
• To submit a service request, visit Cisco Support.
• To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
• To obtain general networking, training, and certification titles, visit Cisco Press.
• To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.
# New and Changed Information

The following table provides an overview of the significant changes made to this configuration guide. The table does not provide an exhaustive list of all changes made to this guide or all new features in a particular release.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Release</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCAM Carving</td>
<td>Enhancements to the TCAM carving feature to support reload of a switch after committing a template.</td>
<td>7.1(4)N1(1)</td>
<td>Configuring TCAM Carving</td>
</tr>
<tr>
<td>Port security</td>
<td>Minor enhancements to the port security feature.</td>
<td>7.1(4)N1(1)</td>
<td>Configuring Port Security</td>
</tr>
<tr>
<td>Sup-region TCAM Monitoring</td>
<td>The Sup-region Ternary Content-Addressable Memory (TCAM) Monitoring feature is a monitoring mechanism that enables detection, reporting and correction of sup-region TCAM entry corruption.</td>
<td>7.1(4)N1(1)</td>
<td>Configuring Sup-region TCAM Monitoring</td>
</tr>
<tr>
<td>Lightweight DHCPv6 Relay Agent</td>
<td>Added the support for the Lightweight DHCPv6 Relay Agent.</td>
<td>7.3(0)N1(1)</td>
<td>Configuring DHCP Snooping</td>
</tr>
<tr>
<td>Object Group ACLs</td>
<td>Added the support for the object group ACLs.</td>
<td>7.3(0)N1(1)</td>
<td>Configuring Access Control Lists</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Release</td>
<td>Where Documented</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Login Block Per User</td>
<td>Added support for login block per user.</td>
<td>7.3(0)N1(1)</td>
<td>Configuring Authentication, Authorization, and Accounting</td>
</tr>
<tr>
<td>Dynamic ARP Inspection Enhancement</td>
<td>Enhancements to the dynamic ARP inspection feature.</td>
<td>7.1(0)N1(1)</td>
<td>Configuring Dynamic ARP Inspection</td>
</tr>
<tr>
<td>Cisco TrustSec</td>
<td>The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices.</td>
<td>7.0(1)N1(1)</td>
<td>Configuring Cisco TrustSec</td>
</tr>
</tbody>
</table>
Overview

The Cisco NX-OS software supports security features that can protect your network against degradation or failure and also against data loss or compromise resulting from intentional attacks and from unintended but damaging mistakes by well-meaning network users.

- Authentication, Authorization, and Accounting, on page 3
- RADIUS and TACACS+ Security Protocols, on page 4
- SSH and Telnet, on page 4
- IP ACLs, on page 4

Authentication, Authorization, and Accounting

Authentication, authorization, and accounting (AAA) is an architectural framework for configuring a set of three independent security functions in a consistent, modular manner.

**Authentication**

Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol that you select, encryption. Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods and then applying that list to various interfaces.

**Authorization**

Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights, with the appropriate user. AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared with the information contained in a database for a given user, and the result is returned to AAA to determine the user’s actual capabilities and restrictions.

**Accounting**

Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables you to track the services that users are accessing, as well as the amount of network resources that they are consuming.
You can configure authentication outside of AAA. However, you must configure AAA if you want to use RADIUS or TACACS+, or if you want to configure a backup authentication method.

### RADIUS and TACACS+ Security Protocols

AAA uses security protocols to administer its security functions. If your router or access server is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS or TACACS+ security server.

The chapters in this guide describe how to configure the following security server protocols:

**RADIUS**

A distributed client/server system implemented through AAA that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

**TACACS+**

A security application implemented through AAA that provides a centralized validation of users who are attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. TACACS+ provides for separate and modular authentication, authorization, and accounting facilities.

### SSH and Telnet

You can use the Secure Shell (SSH) server to enable an SSH client to make a secure, encrypted connection to a Cisco NX-OS device. SSH uses strong encryption for authentication. The SSH server in the Cisco NX-OS software can interoperate with publicly and commercially available SSH clients.

The SSH client in the Cisco NX-OS software works with publicly and commercially available SSH servers.

The Telnet protocol enables TCP/IP connections to a host. Telnet allows a user at one site to establish a TCP connection to a login server at another site and then passes the keystrokes from one device to the other. Telnet can accept either an IP address or a domain name as the remote device address.

### IP ACLs

IP ACLs are ordered sets of rules that you can use to filter traffic based on IPv4 information in the Layer 3 header of packets. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When the Cisco NX-OS software determines that an IP ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether a packet is permitted or denied, or if there is no match, the Cisco NX-OS software applies the applicable default rule. The Cisco NX-OS software continues processing packets that are permitted and drops packets that are denied.
Information About AAA

AAA Security Services

The authentication, authorization, and accounting (AAA) features allows you to verify the identity of, grant access to, and track the actions of users who manage Cisco Nexus devices. The Cisco Nexus device supports Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control device Plus (TACACS+) protocols.

Based on the user ID and password that you provide, the switches perform local authentication or authorization using the local database or remote authentication or authorization using one or more AAA servers. A preshared secret key provides security for communication between the switch and AAA servers. You can configure a common secret key for all AAA servers or for only a specific AAA server.

AAA security provides the following services:

- **Authentication**—Identifies users, including login and password dialog, challenge and response, messaging support, and, encryption depending on the security protocol that you select.

- **Authorization**—Provides access control.

Authorization to access a Cisco Nexus device is provided by attributes that are downloaded from AAA servers. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user.
Benefits of Using AAA

AAA provides the following benefits:

- Increased flexibility and control of access configuration
- Scalability
- Standardized authentication methods, such as RADIUS and TACACS+
- Multiple backup devices

Remote AAA Services

Remote AAA services provided through RADIUS and TACACS+ protocols have the following advantages over local AAA services:

- User password lists for each switch in the fabric are easier to manage.
- AAA servers are already deployed widely across enterprises and can be easily used for AAA services.
- The accounting log for all switches in the fabric can be centrally managed.
- User attributes for each switch in the fabric are easier to manage than using the local databases on the switches.

AAA Server Groups

You can specify remote AAA servers for authentication, authorization, and accounting using server groups. A server group is a set of remote AAA servers that implement the same AAA protocol. A server group provides for failover servers if a remote AAA server fails to respond. If the first remote server in the group fails to respond, the next remote server in the group is tried until one of the servers sends a response. If all the AAA servers in the server group fail to respond, that server group option is considered a failure. If required, you can specify multiple server groups. If a switch encounters errors from the servers in the first group, it tries the servers in the next server group.

AAA Service Configuration Options

On Cisco Nexus devices, you can have separate AAA configurations for the following services:

- User Telnet or Secure Shell (SSH) login authentication
- Console login authentication
• User management session accounting

The following table lists the CLI commands for each AAA service configuration option.

Table 2: AAA Service Configuration Commands

<table>
<thead>
<tr>
<th>AAA Service Configuration Option</th>
<th>Related Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet or SSH login</td>
<td><code>aaa authentication login default</code></td>
</tr>
<tr>
<td>Console login</td>
<td><code>aaa authentication login console</code></td>
</tr>
<tr>
<td>User session accounting</td>
<td><code>aaa accounting default</code></td>
</tr>
</tbody>
</table>

You can specify the following authentication methods for the AAA services:

• RADIUS server groups—Uses the global pool of RADIUS servers for authentication.
• Specified server groups—Uses specified RADIUS or TACACS+ server groups for authentication.
• Local—Uses the local username or password database for authentication.
• None—Uses only the username.

Note

If the method is for all RADIUS servers, instead of a specific server group, the Cisco Nexus devices choose the RADIUS server from the global pool of configured RADIUS servers in the order of configuration. Servers from this global pool are the servers that can be selectively configured in a RADIUS server group on the Cisco Nexus devices.

The following table describes the AAA authentication methods that you can configure for the AAA services.

Table 3: AAA Authentication Methods for AAA Services

<table>
<thead>
<tr>
<th>AAA Service</th>
<th>AAA Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console login authentication</td>
<td>Server groups, local, and none</td>
</tr>
<tr>
<td>User login authentication</td>
<td>Server groups, local, and none</td>
</tr>
<tr>
<td>User management session accounting</td>
<td>Server groups and local</td>
</tr>
</tbody>
</table>

Note

For console login authentication, user login authentication, and user management session accounting, the Cisco Nexus devices try each option in the order specified. The local option is the default method when other configured options fail.

Authentication and Authorization Process for User Logins

The authentication and authorization process for user login is as occurs:
• When you log in to the required Cisco Nexus device, you can use the Telnet, SSH, Fabric Manager or Device Manager, or console login options.

• When you have configured the AAA server groups using the server group authentication method, the Cisco Nexus device sends an authentication request to the first AAA server in the group as follows:
  If the AAA server fails to respond, then the next AAA server is tried and so on until the remote server responds to the authentication request.
  If all AAA servers in the server group fail to respond, the servers in the next server group are tried.
  If all configured methods fail, the local database is used for authentication.

• If a Cisco Nexus device successfully authenticates you through a remote AAA server, the following conditions apply:
  If the AAA server protocol is RADIUS, user roles specified in the cisco-av-pair attribute are downloaded with an authentication response.
  If the AAA server protocol is TACACS+, another request is sent to the same server to get the user roles specified as custom attributes for the shell.

• If your username and password are successfully authenticated locally, the Cisco Nexus device logs you in and assigns you the roles configured in the local database.

The following figure shows a flowchart of the authentication and authorization process.

Figure 1: Authentication and Authorization Flow for User Login

In the figure, "No more servers left" means that there is no response from any server within this server group.
Prerequisites for Remote AAA

Remote AAA servers have the following prerequisites:

• At least one RADIUS or TACACS+ server must be IP reachable.
• The Cisco Nexus device is configured as a client of the AAA servers.
• The preshared secret key is configured on the Cisco Nexus device and on the remote AAA servers.
• The remote server responds to AAA requests from the Cisco Nexus device.

Guidelines and Limitations for AAA

The Cisco Nexus devices do not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally. If an all numeric username exists on an AAA server and is entered during a login, the Cisco Nexus device still logs in the user.

Caution: You should not create user accounts with usernames that are all numeric.

Default AAA Settings

The following table lists the default settings for AAA parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console authentication method</td>
<td>local</td>
</tr>
<tr>
<td>Default authentication method</td>
<td>local</td>
</tr>
<tr>
<td>Login authentication failure messages</td>
<td>Disabled</td>
</tr>
<tr>
<td>MSCHAP authentication</td>
<td>Disabled</td>
</tr>
<tr>
<td>Default accounting method</td>
<td>local</td>
</tr>
<tr>
<td>Accounting log display length</td>
<td>250 KB</td>
</tr>
</tbody>
</table>
Configuring AAA

Configuring Console Login Authentication Methods

The authentication methods include the following:

- Global pool of RADIUS servers
- Named subset of RADIUS or TACACS+ servers
- Local database on the Cisco Nexus device.
- Username only none

The default method is local.

Note

The group radius and group server-name forms of the aaa authentication command are used for a set of previously defined RADIUS servers. Use the radius server-host command to configure the host servers. Use the aaa group server radius command to create a named group of servers.

Before you configure console login authentication methods, configure RADIUS or TACACS+ server groups as needed.

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>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures login authentication methods for the console.</td>
</tr>
</tbody>
</table>
| switch(config)# aaa authentication login console {group group-list [none] | local | none} | The group-list argument consists of a space-delimited list of group names. The group names are the following:
  - radius — Uses the global pool of RADIUS servers for authentication.
  - named-group — Uses a named subset of TACACS+ or RADIUS servers for authentication.

The local method uses the local database for authentication. The none method uses the username only.

The default console login method is local, which is used when no methods are configured or when all of the configured methods fail to respond. |
### Purpose

**Command or Action** | **Purpose**
--- | ---
**Step 3** | switch(config)# exit

Exits global configuration mode.

**Step 4** | (Optional) switch# show aaa authentication

Displays the configuration of the console login authentication methods.

**Step 5** | (Optional) switch# copy running-config startup-config

Copies the running configuration to the startup configuration.

### Example

This example shows how to configure authentication methods for the console login:

```
switch# configure terminal
switch(config)# aaa authentication login console group radius
switch(config)# exit
switch# show aaa authentication
switch# copy running-config startup-config
```

### Configuring Default Login Authentication Methods

The default method is local.

Before you configure default login authentication methods, configure RADIUS or TACACS+ server groups as needed.

### Procedure

**Command or Action** | **Purpose**
--- | ---
**Step 1** | switch# configure terminal

Enters global configuration mode.

**Step 2** | switch(config)# aaa authentication login default {group group-list [none] | local | none}

Configures the default authentication methods.

The `group-list` argument consists of a space-delimited list of group names. The group names are the following:

- `radius` — Uses the global pool of RADIUS servers for authentication.
- `named-group` — Uses a named subset of TACACS+ or RADIUS servers for authentication.

The `local` method uses the local database for authentication. The `none` method uses the username only.

The default login method is `local`, which is used when no methods are configured or when all of the configured methods do not respond.
Enabling Login Authentication Failure Messages

When you log in, the login is processed by the local user database if the remote AAA servers do not respond. If you have enabled the displaying of login failure messages, the following message is displayed:

Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 switch(config)# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 switch(config)# aaa authentication login error-enable</td>
<td>Enables login authentication failure messages. The default is disabled.</td>
</tr>
<tr>
<td>Step 3 switch(config)# exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Step 4 (Optional) switch# show aaa authentication</td>
<td>Displays the login failure message configuration.</td>
</tr>
<tr>
<td>Step 5 (Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Configuring Console Authorization Commands

The authorization methods include the following:

- Named subset of TACACS+ servers
- Local database on the Cisco Nexus device.
- Username only **none**

The default method is local.

Before you configure console authorization commands, configure TACACS+ server groups as needed.

Procedure

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

Configures authorization for the console.

```
switch(config)# aaa authorization commands console {group group-list [none] | local | none}
```

**Purpose**

Confirms the user's role and access to the console.

**Step 2**

The `group-list` argument consists of a space-delimited list of group name. The group name is:

- `named-group` — Uses a named subset of TACACS+ servers for authorization.
- `local` — Uses the local database for authorization.
- `none` — Uses the username only.

The default console authorization is `local`, which is used when no methods are configured or when all of the configured methods fail to respond.

```
switch(config)# exit
```

**Step 3**

Exits global configuration mode.

```
(Optional) switch# show aaa authorization
```

**Step 4**

Displays the configuration of the console authorization commands.

```
(Optional) switch# copy running-config startup-config
```

**Step 5**

Copies the running configuration to the startup configuration.

### Example

This example shows how to configure the console authorization commands:

```
switch# configure terminal
switch(config)# aaa authorization commands console group tacacs+
switch(config)# exit
switch# show aaa authorization
switch# copy running-config startup-config
```

### Enabling MSCHAP Authentication

Microsoft Challenge Handshake Authentication Protocol (MSCHAP) is the Microsoft version of CHAP. You can use MSCHAP for user logins to a Cisco Nexus device through a remote authentication server (RADIUS or TACACS+).

By default, the Cisco Nexus device uses Password Authentication Protocol (PAP) authentication between the switch and the remote server. If you enable MSCHAP, you must configure your RADIUS server to recognize the MSCHAP vendor-specific attributes (VSAs).

The following table describes the RADIUS VSAs required for MSCHAP.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures authorization for the console.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Displays the configuration of the console authorization commands.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

---

**Enabling MSCHAP Authentication**

Microsoft Challenge Handshake Authentication Protocol (MSCHAP) is the Microsoft version of CHAP. You can use MSCHAP for user logins to a Cisco Nexus device through a remote authentication server (RADIUS or TACACS+).

By default, the Cisco Nexus device uses Password Authentication Protocol (PAP) authentication between the switch and the remote server. If you enable MSCHAP, you must configure your RADIUS server to recognize the MSCHAP vendor-specific attributes (VSAs).

The following table describes the RADIUS VSAs required for MSCHAP.
Table 5: MSCHAP RADIUS VSAs

<table>
<thead>
<tr>
<th>Vendor-ID Number</th>
<th>Vendor-Type Number</th>
<th>VSA</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>311</td>
<td>11</td>
<td>MSCHAP-Challenge</td>
<td>Contains the challenge sent by an AAA server to an MSCHAP 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 an MSCHAP user in response to the challenge. It is only used in Access-Request packets.</td>
</tr>
</tbody>
</table>

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 switch(config)# aaa authentication login mschap enable</td>
<td>Enables MS-CHAP authentication. The default is disabled.</td>
</tr>
<tr>
<td>Step 3 switch(config)# exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Step 4 (Optional) switch# show aaa authentication login mschap</td>
<td>Displays the MS-CHAP configuration.</td>
</tr>
<tr>
<td>Step 5 (Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Configuring AAA Accounting Default Methods

The Cisco Nexus device supports TACACS+ and RADIUS methods for accounting. The switches report user activity to TACACS+ or RADIUS security servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the AAA server.

When you activate AAA accounting, the Cisco Nexus device reports these attributes as accounting records, which are then stored in an accounting log on the security server.

You can create default method lists defining specific accounting methods, which include the following:

- RADIUS server group—Uses the global pool of RADIUS servers for accounting.
- Specified server group—Uses a specified RADIUS or TACACS+ server group for accounting.
- Local—Uses the local username or password database for accounting.

Note

If you have configured server groups and the server groups do not respond, by default, the local database is used for authentication.
**Before you begin**

Before you configure AAA accounting default methods, configure RADIUS or TACACS+ server groups as needed.

**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>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

**Step 2**

switch(config)# aaa accounting default {group group-list | local}

Configures the default accounting method. One or more server group names can be specified in a space-separated list.

The `group-list` argument consists of a space-delimited list of group names. The group names are the following:

- **radius** — Uses the global pool of RADIUS servers for accounting.
- **named-group** — Uses a named subset of TACACS+ or RADIUS servers for accounting.

The `local` method uses the local database for accounting.

The default method is **local**, which is used when no server groups are configured or when all the configured server group do not respond.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>switch(config)# exit</td>
<td>Exits configuration mode.</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>(Optional) switch# show aaa accounting</td>
<td>Displays the configuration AAA accounting default methods.</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>(Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Using AAA Server VSAs**

**VSAs**

You can use vendor-specific attributes (VSAs) to specify the Cisco Nexus device user roles and SNMPv3 parameters on AAA servers.

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating VSAs between the network access server and the RADIUS server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option is vendor type 1, which is named cisco-av-pair. The value is a string with the following format:
The protocol is a Cisco attribute for a particular type of authorization, separator is an equal sign (=) for mandatory attributes, and an asterisk (*) indicates optional attributes.

When you use RADIUS servers for authentication on a Cisco Nexus device, the RADIUS protocol directs the RADIUS server to return user attributes, such as authorization information, with authentication results. This authorization information is specified through VSAs.

**VSA Format**

The following VSA protocol options are supported by the Cisco Nexus device:

- **Shell**—Used in access-accept packets to provide user profile information.
- **Accounting**—Used in accounting-request packets. If a value contains any white spaces, put it within double quotation marks.

The following attributes are supported by the Cisco Nexus device:

- **roles**—Lists all the roles assigned to the user. The value field is a string that stores the list of group names delimited by white space.
- **accountinginfo**—Stores additional accounting information in addition to the attributes covered by a standard RADIUS accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the RADIUS client on the switch, and it can only be used with the accounting protocol-related PDUs.

**Specifying Switch User Roles and SNMPv3 Parameters on AAA Servers**

You can use the VSA cisco-av-pair on AAA servers to specify user role mapping for the Cisco Nexus device using this format:

```
shell:roles="roleA roleB ...
```

If you do not specify the role option in the cisco-av-pair attribute, the default user role is network-operator.

---

**Note**


You can also specify your SNMPv3 authentication and privacy protocol attributes as follows:

```
shell:roles="roleA roleB ..." snmpv3:auth=SHA priv=AES-128
```

The SNMPv3 authentication protocol options are SHA and MD5. The privacy protocol options are AES-128 and DES. If you do not specify these options in the cisco-av-pair attribute, MD5 and DES are the default authentication protocols.

For additional information, see the Configuring User Accounts and RBAC chapter in the System Management Configuration Guide for your Cisco Nexus device.

**Secure Login Enhancements**

The following secure login enhancements are supported in Cisco NX-OS:
Configuring Login Parameters

Use this task to configure your Cisco NX-OS device for login parameters that help detect suspected DoS attacks and slow down dictionary attacks.

All login parameters are disabled by default. You must enter the `login block-for` command, which enables default login functionality, before using any other login commands. After the `login block-for` command is enabled, the following default is enforced:

- All login attempts made through Telnet or SSH are denied during the quiet period; that is, no ACLs are exempt from the login period until the `login quiet-mode access-class` command is entered.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>[no] login block-for seconds attempts tries within seconds</code></td>
<td>Configures your Cisco NX-OS device for login parameters that help provide DoS detection.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# login block-for 100 attempts 2 within 100</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>This command must be issued before any other login command can be used.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>`[no] login quiet-mode access-class {acl-name</td>
<td>acl-number}`</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# login quiet-mode access-class myacl</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>exit</code></td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>show login failures</code></td>
<td>Displays login parameters.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# show login</td>
<td></td>
</tr>
<tr>
<td>• failures</td>
<td>Displays information related only to failed login attempts.</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Examples for Login Parameters

Setting Login Parameters Example

The following example shows how to configure your switch to enter a 100 second quiet period if 15 failed login attempts is exceeded within 100 seconds; all login requests are denied during the quiet period except hosts from the ACL "myacl."

Switch(config)# login block-for 100 attempts 15 within 100
Switch(config)# login quiet-mode access-class myacl

Showing Login Parameters Example

The following sample output from the show login command verifies that no login parameters have been specified:

Switch# show login

No Quiet-Mode access list has been configured, default ACL will be applied.

Switch is enabled to watch for login Attacks.
If more than 2 login failures occur in 45 seconds or less, logins will be disabled for 70 seconds.

Switch presently in Normal-Mode.
Current Watch Window remaining time 10 seconds.
Present login failure count 0.

The following sample output from the show login failures command shows all failed login attempts on the switch:

Switch# show login failures

Information about last 20 login failures with the device.
--------------------------------------------------------------------------------
Username | Line | Source | Appname
--------------------------------------------------------------------------------
admin    | pts/0 | bgl-ads-728.cisco.com | login
admin    | pts/0 | bgl-ads-728.cisco.com | login
--------------------------------------------------------------------------------

The following sample output from the show login failures command verifies that no information is presently logged:

Switch# show login failures
*** No logged failed login attempts with the device.***

Configuring Login Block Per User

The Login Block Per User feature helps detect suspected Denial of Service (DoS) attacks and to slow down dictionary attacks. This feature is applicable only for local users. Use this task to configure login parameters to block an user after failed login attempts.
### Configuration Examples for Login Block Per User

#### Setting Parameters for Login Block Per User

The following example shows how to configure the login parameters to block a user for 300 seconds when five login attempts fail within a period of 60 seconds:

```
switch(config)# aaa authentication rejected 5 in 60 ban 300
```

#### Showing Login Parameters

The following example shows the login parameters configured for a switch:

```
switch# show running config
```

```
Restricting Sessions Per User—Per User Per Login

Use this task to restrict the maximum sessions per user.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>[no] user max-logins max-logins</code></td>
<td>Restricts the maximum sessions per user.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# user max-logins 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Passphrase Length

Use this task to configure the maximum and minimum passphrase length.

switch# show run | i rejected
aaa authentication rejected 5 in 60 ban 300

Showing Blocked Local Users

The following example shows the blocked local users:

switch# show aaa local user blocked
Local-user            State
testuser             Watched (till 11:34:42 IST Feb 5 2015)

Clearing Blocked Local Users

The following example shows how to clear the blocked local user testuser:

switch# clear aaa local user blocked username testuser
## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> userpassphrase {min-length value | max-length value} | min-length value max-length value</td>
<td>Configures the user passphrase length. The range of minimum passphrase length values are from 8 to 127. The range of maximum passphrase length values are from 80 to 127. The default minimum passphrase length is 8 and the default maximum passphrase length is 127.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# userpassphrase max-length 127</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> no userpassphrase {min-length</td>
<td>max-length</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# no userpassphrase max-length</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show userpassphrase {min-length</td>
<td>max-length</td>
</tr>
<tr>
<td><strong>Example:</strong> switch# show userpassphrase length</td>
<td></td>
</tr>
</tbody>
</table>

## Configuring Passphrase Time Values

You can configure the following passphrase time values for a user:

- **Lifetime** – Life time of a passphrase in days. After the passphrase expires, the user is prompted to change the passphrase upon first login.

- **Gracetime** – Grace time of a passphrase in days. Gracetime is the number of days of inactivity after a passphrase has expired before an account is locked.

- **Warntime** – Warning time of the expiry of a passphrase in days. Warntime is the number of days prior to a passphrase expiring, when a user is warned that the user's passphrase is about to expire.

The default time values are 99999 days for lifetime, 14 days for warntime, and 3 days for gracetime. The value 99999 indicates that a user's passphrase never expires by default.
By default, an extra configuration is added to the running configuration for every user except 'admin'. This indicates a user's passphrase time values. By default, the extra configuration displays the default passphrase time values for users.

### 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></td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>username username passphrase { Florian lifetime</td>
<td>warnetime</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# username test-user passphrase lifetime 990</td>
<td>Configures passphrase time values for a user. Note that this step can be performed only by a network-admin.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) no username username passphrase { Florian lifetime</td>
<td>warnetime</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# no username test-user passphrase lifetime</td>
<td>Resets passphrase time value to default values for a user. Note that this step can be performed only by a network-admin.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) userpassphrase { default-lifetime</td>
<td>default-warnetime</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# userpassphrase default-lifetime 990</td>
<td>Updates default passphrase time values. Note that this step can be performed only by a network-admin.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) no userpassphrase { default-lifetime</td>
<td>default-warnetime</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# no userpassphrase default-lifetime</td>
<td>Resets the configured default values to the initial default values. Note that this step can be performed only by a network-admin.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) username username expire-userpassphrase</td>
<td>Sets any userpassphrase to expire immediately. When you try to log in after a passphrase</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>expires, you are prompted to enter and create a new password after entering the old password correctly. Note that this step can be performed only by an admin.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 7**
Example:
```
switch(config)# exit
```
Exits to privileged EXEC mode.

**Step 8**
Example:
```
switch# show userpassphrase {default-lifetime | default-warntime | default-gracetime | timevalues}
```
Displays the passphrase time values.

**Step 9**
Example:
```
switch# show username john passphrase timevalues
```
Displays the passphrase lifetime, warning time, and grace time for a specific user.

**Step 10**
Example:
```
switch# show running-config
```
Displays the configured values.

## Configuring Passphrase Time Values

The following example shows how to configure passphrase time values for test-user.
```
switch(config)# username test-user passphrase lifetime 365 warntime 10 gracetime 5
switch(config)# show username test-user passphrase timevalues
Last passphrase change(Y-M-D): 2016-01-28
Passphrase lifetime: 365 days after last passphrase change
Passphrase warning time starts: 10 days before passphrase lifetime
Passphrase Gracetime ends: 5 days after passphrase lifetime
```
```
switch# show running-config
!Command: show running-config
!Time: Mon Nov 30 02:32:51 2015
version 7.3(0)N1(1)
hostname switch
role name test
username admin password 5 5$0sCUIUZQm$5fXdGj90e9yXv1XeuY9qResKmLGKQtn8Tj6ab4s4IcVA role network-admin username test-user password 5 5$c9Gmvm8E$a0SQ1X7vfphlJ6WeRQl3COPy6TlpiDjhWcF6kYi4hg6 expire 1970-01-01 role network-operator
```
Locking User Accounts

As an admin, you can lock or unlock any user account.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>[no] username username lock-user-account</td>
<td>Locks the specified user account. Use the no form of this command to unlock a user account.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# username john lock-user-account</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>(Optional) unlock locked-users</td>
<td>Unlocks all the locked user accounts.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# unlock locked-users</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# exit</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>show locked-users</td>
<td>Displays all the locked users.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# show locked-users</td>
<td></td>
</tr>
</tbody>
</table>

Logging Invalid Usernames

As an admin, you can ensure non-logging or logging of invalid usernames in logs during an authentication failure. By default, invalid usernames during authentication failures are not logged. Any username that does not pass authentication is considered as an invalid username and it is not logged, because when a password is entered in the username field by mistake, it can get logged. This feature can be used to mitigate the risk of logging passwords.

**Procedure**

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

username test-user passphrase lifetime 365 warntime 10 gracetime 5
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch# configure terminal</code></td>
<td>Enables the logging of invalid usernames during an authentication failure. Use the <code>no</code> form of this command to disable the logging of invalid usernames.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>[no] aaa authentication login invalid-username-log</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# aaa authentication login invalid-username-log</code></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch(config)# exit</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Displays whether logging invalid names is enabled.</td>
</tr>
<tr>
<td><code>show aaa authentication login invalid-username-log</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>switch# show aaa authentication login invalid-username-log</code></td>
</tr>
</tbody>
</table>

**Changing Password**

Use this task to change the password.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Enter global configuration mode:</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

To change the password, perform one of the following:

- Authenticate with the old password and then enter the new password:

  `switch(config)# change-password`

  **Note** By default, `password secure-mode` is enabled. So, users must use the old password for authentication before changing the password. An admin user can disable password secure-mode by using the `no password secure-mode` command. This enables users to change password without authenticating with the old password by using the `username username password new_password` command.

  - If password secure-mode is enabled, an admin user can still use the `username` command to change password:
  
    `switch(config)# username admin password new-password role role-name`

  **Note** If password secure-mode is disabled, any user can use the `username` command to change the password.
Enabling the Password Prompt for User Name

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>[no] password prompt username</code></td>
<td>Enables the login knob. If this command is enabled and the user enters the <code>username</code> command without the password option, then the password is prompted. The password accepts hidden characters. Use the <code>no</code> form of this command to disable the login knob.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# password prompt username</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

Support over SHA-256 Algorithm for Verifying OS Integrity

Use the `show file bootflash:/ sha256sum` command to display the sha256sum of the file. The sample output for this command is shown below:

```
Switch# show file bootflash:/ sha256sum
```
Configuring Share Key Value for using RADIUS/TACACS+

The shared secret you configure for remote authentication and accounting must be hidden. For the `radius-server key` and `tacacs-server key` commands, a separate command to generate encrypted shared secret can be used.

### 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: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>generate type7_encrypted_secret</code></td>
<td>Configures RADIUS and TACACS shared secret with key type 7. While generating an encrypted shared secret, user input is hidden.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# generate type7_encrypted_secret</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>You can generate encrypted equivalent of plain text separately and can configure the encrypted shared secret later.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>exit</code></td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Monitoring and Clearing the Local AAA Accounting Log

The Cisco Nexus device maintains a local log for the AAA accounting activity.

### 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>switch# show accounting log [size] [start-time year month day hh : mm : ss]</code></td>
<td>Displays the accounting log contents. By default, the command output contains up to 250,000 bytes of the accounting log. You can use the size argument to limit command output. The range is from 0 to 250000 bytes. You can also specify a start time for the log output.</td>
</tr>
<tr>
<td>Step 2</td>
<td>(Optional) <code>switch# clear accounting log</code></td>
<td>Clears the accounting log contents.</td>
</tr>
</tbody>
</table>
Verifying the AAA Configuration

To display AAA information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show aaa accounting</td>
<td>Displays AAA accounting configuration.</td>
</tr>
<tr>
<td>show aaa authentication [login {error-enable</td>
<td>Displays AAA authentication information.</td>
</tr>
<tr>
<td>mschap}]</td>
<td></td>
</tr>
<tr>
<td>show aaa authorization</td>
<td>Displays AAA authorization information.</td>
</tr>
<tr>
<td>show aaa groups</td>
<td>Displays the AAA server group configuration.</td>
</tr>
<tr>
<td>show running-config aaa [all]</td>
<td>Displays the AAA configuration in the running</td>
</tr>
<tr>
<td></td>
<td>configuration.</td>
</tr>
<tr>
<td>show startup-config aaa</td>
<td>Displays the AAA configuration in the startup</td>
</tr>
<tr>
<td></td>
<td>configuration.</td>
</tr>
</tbody>
</table>

Configuration Examples for AAA

The following example shows how to configure AAA:

```
switch(config)# aaa authentication login default group radius
switch(config)# aaa authentication login console group radius
switch(config)# aaa accounting default group radius
```
CHAPTER 4

Configuring RADIUS

This chapter contains the following sections:

- Information About RADIUS, on page 29
- Prerequisites for RADIUS, on page 32
- Guidelines and Limitations for RADIUS, on page 32
- Default Settings for RADIUS, on page 32
- Configuring RADIUS Servers, on page 33
- Verifying the RADIUS Configuration, on page 44
- Displaying RADIUS Server Statistics, on page 44
- Clearing RADIUS Server Statistics, on page 44
- Configuration Examples for RADIUS, on page 45

Information About RADIUS

The Remote Access Dial-In User Service (RADIUS) distributed client/server system allows you to secure networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco Nexus devices and send authentication and accounting requests to a central RADIUS server that contains all user authentication and network service access information.

RADIUS Network Environments

RADIUS can be implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

You can use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor network devices, each supporting RADIUS.
  
  For example, network devices from several vendors can use a single RADIUS server-based security database.

- Networks already using RADIUS.
  
  You can add a Cisco Nexus device with RADIUS to the network. This action might be the first step when you make a transition to an AAA server.

- Networks that require resource accounting.
You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use a freeware-based version of the RADIUS access control and accounting software to meet special security and billing needs.

- Networks that support authentication profiles.

Using the RADIUS server in your network, you can configure AAA authentication and set up per-user profiles. Per-user profiles enable the Cisco Nexus device to manage ports using their existing RADIUS solutions and to efficiently manage shared resources to offer different service-level agreements.

**Information About RADIUS Operations**

When a user attempts to log in and authenticate to a Cisco Nexus device using RADIUS, the following process occurs:

1. The user is prompted for and enters 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 not authenticated and is prompted to reenter the username and password, or access is denied.
   - CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.
   - CHANGE PASSWORD—A request is issued by the RADIUS server, asking the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

- Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IPv4 or IPv6 address, access list, and user timeouts.

**RADIUS Server Monitoring**

An unresponsive RADIUS server can cause delay in processing of AAA requests. You can configure the switch to periodically monitor a RADIUS server to check whether it is responding (or alive) to save time in processing AAA requests. The switch marks unresponsive RADIUS servers as dead and does not send AAA requests to any dead RADIUS servers. The switch periodically monitors the dead RADIUS servers and brings them to the alive state once they respond. This process verifies that a RADIUS server is in a working state before real AAA requests are sent to the server. Whenever a RADIUS server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the switch displays an error message that a failure is taking place.
The following figure shows the different RADIUS server states:

*Figure 2: RADIUS Server States*

```
Vendor-Specific Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific attributes (VSAs) between the network access server and the RADIUS server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option is vendor type 1, which is named cisco-av-pair. The value is a string with the following format:

```
protocol : attribute separator value *
```

The protocol is a Cisco attribute for a particular type of authorization, the separator is an equal sign (=) for mandatory attributes, and an asterisk (*) indicates optional attributes.

When you use RADIUS servers for authentication on a Cisco Nexus device, the RADIUS protocol directs the RADIUS server to return user attributes, such as authorization information, with authentication results. This authorization information is specified through VSAs.

The following VSA protocol options are supported by the Cisco Nexus device:

- **Shell**—Used in access-accept packets to provide user profile information.

- **Accounting**—Used in accounting-request packets. If a value contains any white spaces, you should enclose the value within double quotation marks.

The Cisco Nexus device supports the following attributes:

- **roles**—Lists all the roles to which the user belongs. The value field is a string that lists the role names delimited by white spaces.
• accountinginfo—Stores accounting information in addition to the attributes covered by a standard RADIUS accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the RADIUS client on the switch. It can be used only with the accounting protocol data units (PDUs).

Prerequisites for RADIUS

RADIUS has the following prerequisites:

• You must obtain IPv4 or IPv6 addresses or hostnames for the RADIUS servers.
• You must obtain preshared keys from the RADIUS servers.
• Ensure that the Cisco Nexus device is configured as a RADIUS client of the AAA servers.

Guidelines and Limitations for RADIUS

RADIUS has the following configuration guidelines and limitations:

• You can configure a maximum of 64 RADIUS servers on the Cisco Nexus device.
• ASCII (PAP) Authentication is not supported on RADIUS servers.

Default Settings for RADIUS

The following table lists the default settings for RADIUS parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server roles</td>
<td>Authentication and accounting</td>
</tr>
<tr>
<td>Dead timer interval</td>
<td>0 minutes</td>
</tr>
<tr>
<td>Retransmission count</td>
<td>1</td>
</tr>
<tr>
<td>Retransmission timer interval</td>
<td>5 seconds</td>
</tr>
<tr>
<td>Idle timer interval</td>
<td>0 minutes</td>
</tr>
<tr>
<td>Periodic server monitoring username</td>
<td>test</td>
</tr>
<tr>
<td>Periodic server monitoring password</td>
<td>test</td>
</tr>
</tbody>
</table>
Configuring RADIUS Servers

This section describes how to configure RADIUS servers.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Establish the RADIUS server connections to the Cisco Nexus device.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure the preshared secret keys for the RADIUS servers.</td>
</tr>
<tr>
<td>Step 3</td>
<td>If needed, configure RADIUS server groups with subsets of the RADIUS servers for AAA authentication methods.</td>
</tr>
<tr>
<td>Step 4</td>
<td>If needed, configure any of the following optional parameters:</td>
</tr>
<tr>
<td></td>
<td>• Dead-time interval.</td>
</tr>
<tr>
<td></td>
<td>• Allow specification of a RADIUS server at login.</td>
</tr>
<tr>
<td></td>
<td>• Transmission retry count and timeout interval.</td>
</tr>
<tr>
<td></td>
<td>• Accounting and authentication attributes.</td>
</tr>
<tr>
<td>Step 5</td>
<td>If needed, configure periodic RADIUS server monitoring.</td>
</tr>
</tbody>
</table>

Configuring RADIUS Server Hosts

You must configure the IPv4 or IPv6 address or the hostname for each RADIUS server that you want to use for authentication. All RADIUS server hosts are added to the default RADIUS server group. You can configure up to 64 RADIUS servers.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# radius-server host {ipv4-address</td>
</tr>
<tr>
<td></td>
<td>Specifies the IPv4 or IPv6 address or hostname for a RADIUS server.</td>
</tr>
<tr>
<td>Step 3</td>
<td>switch(config)# exit</td>
</tr>
<tr>
<td></td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) switch# show radius-server</td>
</tr>
<tr>
<td></td>
<td>Displays the RADIUS server configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) switch# copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>
Example

The following example shows how to configure host 10.10.1.1 as a RADIUS server:

```bash
switch# configure terminal
switch(config)# radius-server host 10.10.1.1
switch(config)# exit
switch# copy running-config startup-config
```

Configuring RADIUS Global Preshared Keys

You can configure preshared keys at the global level for all servers used by the Cisco Nexus device. A preshared key is a shared secret text string between the switch and the RADIUS server hosts.

**Before you begin**

Obtain the preshared key values for the remote RADIUS servers

**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>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies a preshared key for all RADIUS servers. You can specify a clear text (0) or encrypted (7) preshared key. The default format is clear text. The maximum length is 63 characters. By default, no preshared key is configured.</td>
</tr>
<tr>
<td>switch(config)# radius-server key [0</td>
<td>7] key-value</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>switch(config)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Displays the RADIUS server configuration.</td>
</tr>
<tr>
<td>(Optional) switch# show radius-server</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The preshared keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted preshared keys.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>(Optional) switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

This example shows how to configure preshared keys at the global level for all servers used by the device:
Configuring RADIUS Server Preshared Keys

A preshared key is a shared secret text string between the Cisco Nexus device and the RADIUS server host.

Before you begin

Obtain the preshared key values for the remote RADIUS servers.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>switch(config)# radius-server host</td>
<td>Specifies a preshared key for a specific RADIUS server. You can specify a clear text (0) or encrypted (7) preshared key. The default format is clear text. The maximum length is 63 characters. This preshared key is used instead of the global preshared key.</td>
</tr>
<tr>
<td></td>
<td>{ipv4-address</td>
<td>ipv6-address</td>
</tr>
<tr>
<td>3</td>
<td>switch(config)# exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>(Optional) switch# show radius-server</td>
<td>Displays the RADIUS server configuration. The preshared keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted preshared keys.</td>
</tr>
<tr>
<td>5</td>
<td>(Optional) switch# copy running-config startup-config</td>
<td>Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Example

This example shows how to configure RADIUS preshared keys:

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# copy running-config startup-config
```
Configuring RADIUS Server Groups

You can specify one or more remote AAA servers for authentication using server groups. All members of a group must belong to the RADIUS protocol. The servers are tried in the same order in which you configure them.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>switch (config)# aaa group server radius group-name</td>
<td>Creates a RADIUS server group and enters the RADIUS server group configuration submode for that group. The <code>group-name</code> argument is a case-sensitive, alphanumeric string with a maximum of 127 characters.</td>
</tr>
<tr>
<td>3</td>
<td>switch (config-radius)# server {ipv4-address</td>
<td>ipv6-address</td>
</tr>
<tr>
<td>4</td>
<td>(Optional) switch (config-radius)# deadtime minutes</td>
<td>Configures the monitoring dead time. The default is 0 minutes. The range is from 1 through 1440. <strong>Note</strong> If the dead-time interval for a RADIUS server group is greater than zero (0), that value takes precedence over the global dead-time value.</td>
</tr>
<tr>
<td>5</td>
<td>(Optional) switch(config-radius)# source-interface interface</td>
<td>Assigns a source interface for a specific RADIUS server group. The supported interface types are management and VLAN. <strong>Note</strong> Use the <code>source-interface</code> command to override the global source interface assigned by the <code>ip radius source-interface</code> command.</td>
</tr>
<tr>
<td>6</td>
<td>switch(config-radius)# exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>7</td>
<td>(Optional) switch(config)# show radius-server group [group-name]</td>
<td>Displays the RADIUS server group configuration.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**  
(Optional) `switch(config)# copy running-config startup-config`

**Purpose**  
Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

---

### Example

The following example shows how to configure a RADIUS server group:

```bash
switch# configure terminal
switch (config)# aaa group server radius RadServer
switch (config-radius)# server 10.10.1.1
switch (config-radius)# deadtime 30
switch (config-radius)# use-vrf management
switch (config-radius)# exit
switch (config)# show radius-server group
switch (config)# copy running-config startup-config
```

---

### What to do next

Apply the RADIUS server groups to an AAA service.

### Configuring the Global Source Interface for RADIUS Server Groups

You can configure a global source interface for RADIUS server groups to use when accessing RADIUS servers. You can also configure a different source interface for a specific RADIUS server group.

#### 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>switch# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>switch(config)# ip radius source-interface interface</code></td>
<td>Configures the global source interface for all RADIUS server groups configured on the device. The source interface can be the management or the VLAN interface.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>switch(config)# exit</code></td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) <code>switch# show radius-server</code></td>
<td>Displays the RADIUS server configuration information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) <code>switch# copy running-config startup config</code></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

#### Example

This example shows how to configure the mgmt 0 interface as the global source interface for RADIUS server groups:
Allowing Users to Specify a RADIUS Server at Login

You can allow users to specify a RADIUS server at login.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# radius-server directed-request</td>
<td>Allows users to specify a RADIUS server to send the authentication request when logging in. The default is disabled.</td>
</tr>
<tr>
<td>Step 3</td>
<td>switch(config)# exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) switch# show radius-server directed-request</td>
<td>Displays the directed request configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to allow users to select a RADIUS server when logging in to a network:

```
switch# configure terminal
switch(config)# radius-server directed-request
switch# exit
switch# copy running-config startup-config
```

Configuring the Global RADIUS Transmission Retry Count and Timeout Interval

You can configure a global retransmission retry count and timeout interval for all RADIUS servers. By default, a switch retries transmission to a RADIUS server only once before reverting to local authentication. You can increase this number up to a maximum of five retries per server. The timeout interval determines how long the Cisco Nexus device waits for responses from RADIUS servers before declaring a timeout failure.

**Procedure**

| Step 1        | switch# configure terminal                             | Enters global configuration mode.                                       |
### Configuring the RADIUS Transmission Retry Count and Timeout Interval for a Server

By default, a Cisco Nexus switch retries transmission to a RADIUS server only once before reverting to local authentication. You can increase this number up to a maximum of five retries per server. You can also set a timeout interval that the switch waits for responses from RADIUS servers before declaring a timeout failure.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# radius-server host {ipv4-address</td>
<td>ipv6-address</td>
</tr>
</tbody>
</table>

**Note**

The retransmission count value specified for a RADIUS server overrides the count specified for all RADIUS servers.
### Configuring Accounting and Authentication Attributes for RADIUS Servers

You can specify that a RADIUS server is to be used only for accounting purposes or only for authentication purposes. By default, RADIUS servers are used for both accounting and authentication. You can also specify the destination UDP port numbers where RADIUS accounting and authentication messages should be sent.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> switch# <strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> (Optional) switch(config)# <strong>radius-server host</strong> {ipv4-address</td>
<td>ipv6-address</td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) switch(config)# <strong>radius-server host</strong> {ipv4-address</td>
<td>ipv6-address</td>
</tr>
</tbody>
</table>

---

### Configuring RADIUS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> switch(config)# <strong>radius-server host</strong> {ipv4-address</td>
<td>ipv6-address</td>
</tr>
<tr>
<td><strong>Step 4</strong> switch(config)# <strong>exit</strong></td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) switch# <strong>show radius-server</strong></td>
<td>Displays the RADIUS server configuration.</td>
</tr>
<tr>
<td><strong>Step 6</strong> (Optional) switch# <strong>copy running-config startup-config</strong></td>
<td>Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

---

### Example

This example shows how to set the RADIUS transmission retry count to 3 and the timeout interval to 10 seconds on RADIUS host server server1:

```bash
switch# configure terminal
switch(config)# radius-server host server1 retransmit 3
switch(config)# radius-server host server1 timeout 10
switch(config)# exit
switch# copy running-config startup-config
```
Configuring RADIUS

## Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) switch(config)# radius-server host (ipv4-address</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) switch(config)# radius-server host (ipv4-address</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>switch(config)# exit</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>(Optional) switch(config)# show radius-server</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

### Example

This example shows how to configure accounting and authentication attributes for a RADIUS server:

```plaintext
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 acct-port 2004
switch(config)# radius-server host 10.10.1.1 accounting
switch(config)# radius-server host 10.10.2.2 auth-port 2005
switch(config)# radius-server host 10.10.2.2 authentication
switch # exit
switch # copy running-config startup-config
switch #
```

### Configuring Periodic RADIUS Server Monitoring

You can monitor the availability of RADIUS servers. These parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval during which a RADIUS server receives no requests before the switch sends out a test packet. You can configure this option to test servers periodically.

#### Note

For security reasons, we recommend that you do not configure a test username that is the same as an existing user in the RADIUS database.

The test idle timer specifies the interval during which a RADIUS server receives no requests before the switch sends out a test packet.

The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, the switch does not perform periodic RADIUS server monitoring.
## Configuring RADIUS

### Configuring the Dead-Time Interval

You can configure the dead-time interval for all RADIUS servers. The dead-time interval specifies the time that the Cisco Nexus device waits after declaring a RADIUS server is dead, before sending out a test packet to determine if the server is now alive. The default value is 0 minutes.

### Example

This example shows how to configure RADIUS server host 10.10.1.1 with a username (user1) and password (Ur2Gd2BH) and with an idle timer of 3 minutes and a deadtime of 5 minutes:

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# copy running-config startup-config
```

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>switch(config)# radius-server host {ipv4-address</td>
<td>ipv6-address</td>
</tr>
<tr>
<td>3</td>
<td>switch(config)# radius-server deadtime minutes</td>
<td>Specifies the number of minutes before the switch checks a RADIUS server that was previously unresponsive. The default value is 0 minutes. The valid range is 1 to 1440 minutes.</td>
</tr>
<tr>
<td>4</td>
<td>switch(config)# exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>5</td>
<td>(Optional) switch# show radius-server</td>
<td>Displays the RADIUS server configuration.</td>
</tr>
<tr>
<td>6</td>
<td>(Optional) switch# copy running-config startup-config</td>
<td>Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>
When the dead-time interval is 0 minutes, RADIUS servers are not marked as dead even if they are not responding. You can configure the dead-time interval for a RADIUS server group.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures the dead-time interval. The default value is 0 minutes. The range is from 1 to 1440 minutes.</td>
</tr>
<tr>
<td>switch(config)# radius-server deadtime</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>switch(config)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Displays the RADIUS server configuration.</td>
</tr>
<tr>
<td>(Optional) switch# show radius-server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>(Optional) switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

#### Example

This example shows how to configure a deadtime of 5 minutes for a radius server:

```
switch# configure terminal
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# copy running-config startup-config
```

---

### Manually Monitoring RADIUS Servers or Groups

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Sends a test message to a RADIUS server to confirm availability.</td>
</tr>
<tr>
<td>switch# test aaa server radius {ipv4-address</td>
<td>ipv6-address</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Sends a test message to a RADIUS server group to confirm availability.</td>
</tr>
<tr>
<td>switch# test aaa group group-name username password</td>
<td></td>
</tr>
</tbody>
</table>
Example
This example shows how to send a test message to the RADIUS server and server group to confirm availability:

```
switch# test aaa server radius 10.10.1.1 user 1 Ur2Gd2BH
switch# test aaa group RadGroup user2 As3He3CI
```

Verifying the RADIUS Configuration

To display AAA information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config radius [all]</td>
<td>Displays the RADIUS configuration in the running configuration.</td>
</tr>
<tr>
<td>show startup-config radius</td>
<td>Displays the RADIUS configuration in the startup configuration.</td>
</tr>
<tr>
<td>show radius-server [server-name</td>
<td>ipv4-address</td>
</tr>
</tbody>
</table>

Displaying RADIUS Server Statistics

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>switch# show radius-server statistics {hostname</td>
</tr>
</tbody>
</table>

Clearing RADIUS Server Statistics

You can display the statistics that the Cisco NX-OS device maintains for RADIUS server activity.

Before you begin
Configure RADIUS servers on the Cisco NX-OS device.
## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> (Optional) switch# show radius-server statistics {hostname</td>
<td>ipv4-address</td>
</tr>
<tr>
<td><strong>Step 2</strong> switch# clear radius-server statistics {hostname</td>
<td>ipv4-address</td>
</tr>
</tbody>
</table>

## Configuration Examples for RADIUS

The following example shows how to configure RADIUS:

```bash
switch# configure terminal
switch(config)# radius-server key 7 "ToIkLhPpG"
switch(config)# radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
switch(config-radius)# exit
switch(config-radius)# use-vrf management
```
CHAPTER 5

Configuring TACACS+

This chapter contains the following sections:

- Information About Configuring TACACS+, on page 47
- Prerequisites for TACACS+, on page 49
- Guidelines and Limitations for TACACS+, on page 50
- Default Settings for TACACS+, on page 50
- Configuring TACACS+, on page 50
- Displaying TACACS+ Statistics, on page 60
- Verifying the TACACS+ Configuration, on page 61
- Configuration Examples for TACACS+, on page 61

Information About Configuring TACACS+

The Terminal Access Controller Access Control System Plus (TACACS+) security protocol provides centralized validation of users attempting to gain access to a Cisco Nexus device. TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your Cisco Nexus device are available.

TACACS+ provides for separate authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service (authentication, authorization, and accounting) independently. Each service is associated with 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 TACACS+ client/server protocol uses TCP (TCP port 49) for transport requirements. The Cisco Nexus device provides centralized authentication using the TACACS+ protocol.

TACACS+ Advantages

TACACS+ has the following advantages over RADIUS authentication:

- Provides independent AAA facilities. For example, the Cisco Nexus device can authorize access without authenticating.
- Uses the TCP transport protocol to send data between the AAA client and server, making reliable transfers with a connection-oriented protocol.
 Encrypts the entire protocol payload between the switch and the AAA server to ensure higher data confidentiality. The RADIUS protocol only encrypts passwords.

User Login with TACACS+

When a user attempts a Password Authentication Protocol (PAP) login to a Cisco Nexus device using TACACS+, the following actions occur:

1. When the Cisco Nexus device establishes a connection, it contacts the TACACS+ daemon to obtain the username and password.

   TACACS+ allows an arbitrary conversation between the daemon and the user until the daemon receives enough information to authenticate the user. This action is usually done by prompting for a username and password combination, but may include prompts for other items, such as the user’s mother’s maiden name.

2. The Cisco Nexus device receives one of the following responses from the TACACS+ daemon:
   - ACCEPT — User authentication succeeds and service begins. If the Cisco Nexus device requires user authorization, authorization begins.
   - REJECT — User authentication failed. The TACACS+ daemon either denies further access to the user or prompts the user to retry the login sequence.
   - ERROR — An error occurred at some time during authentication either at the daemon or in the network connection between the daemon and the Cisco Nexus device. If the Cisco Nexus device receives an ERROR response, the switch tries to use an alternative method for authenticating the user.

   The user also undergoes an additional authorization phase, if authorization has been enabled on the Cisco Nexus device. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the Cisco Nexus device again contacts the TACACS+ daemon and it returns an ACCEPT or REJECT authorization response. An ACCEPT response contains attributes that are used to direct the EXEC or NETWORK session for that user and determines the services that the user can access.

   Services include the following:
   - Telnet, rlogin, Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services
   - Connection parameters, including the host or client IP address (IPv4), access list, and user timeouts

Default TACACS+ Server Encryption Type and Preshared Key

You must configure the TACACS+ that is preshared key to authenticate the switch to the TACACS+ server. A preshared key is a secret text string shared between the Cisco Nexus device and the TACACS+ server host. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global preshared secret key for all TACACS+ server configurations on the Cisco Nexus device to use.
You can override the global preshared key assignment by using the `key` option when configuring an individual TACACS+ server.

**TACACS+ Server Monitoring**

An unresponsive TACACS+ server can delay the processing of AAA requests. A Cisco Nexus device can periodically monitor an TACACS+ server to check whether it is responding (or alive) to save time in processing AAA requests. The Cisco Nexus device marks unresponsive TACACS+ servers as dead and does not send AAA requests to any dead TACACS+ servers. The Cisco Nexus device periodically monitors dead TACACS+ servers and brings them to the alive state once they are responding. This process verifies that a TACACS+ server is in a working state before real AAA requests are sent to the server. Whenever an TACACS+ server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Cisco Nexus device displays an error message that a failure is taking place before it can impact performance.

The following figure shows the different TACACS+ server states:

*Figure 3: TACACS+ Server States*

The monitoring interval for alive servers and dead servers are different and can be configured by the user. The TACACS+ server monitoring is performed by sending a test authentication request to the TACACS+ server.

---

**Note**

The monitoring interval for alive servers and dead servers are different and can be configured by the user. The TACACS+ server monitoring is performed by sending a test authentication request to the TACACS+ server.

---

**Prerequisites for TACACS+**

TACACS+ has the following prerequisites:

- You must obtain the IPv4 addresses or hostnames for the TACACS+ servers.
- You must obtain the preshared keys from the TACACS+ servers, if any.
- Ensure that the Cisco Nexus device is configured as a TACACS+ client of the AAA servers.
Guidelines and Limitations for TACACS+

TACACS+ has the following configuration guidelines and limitations:

- You can configure a maximum of 64 TACACS+ servers on the Cisco Nexus device.

Default Settings for TACACS+

The following table lists the default settings for TACACS+ parameters.

Table 7: Default TACACS+ Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS+</td>
<td>Disabled</td>
</tr>
<tr>
<td>Dead-time interval</td>
<td>0 minutes</td>
</tr>
<tr>
<td>Timeout interval</td>
<td>5 seconds</td>
</tr>
<tr>
<td>Idle timer interval</td>
<td>0 minutes</td>
</tr>
<tr>
<td>Periodic server monitoring username</td>
<td>test</td>
</tr>
<tr>
<td>Periodic server monitoring password</td>
<td>test</td>
</tr>
</tbody>
</table>

Configuring TACACS+

TACACS+ Server Configuration Process

This section describes how to configure TACACS+ servers.

Procedure

- **Step 1**  Enable TACACS+.
- **Step 2**  Establish the TACACS+ server connections to the Cisco Nexus device.
- **Step 3**  Configure the preshared secret keys for the TACACS+ servers.
- **Step 4**  If needed, configure TACACS+ server groups with subsets of the TACACS+ servers for AAA authentication methods.
- **Step 5**  If needed, configure any of the following optional parameters:
  - Dead-time interval
• Allow TACACS+ server specification at login
• Timeout interval
• TCP port

Step 6  If needed, configure periodic TACACS+ server monitoring.

Enabling TACACS+

Although by default, the TACACS+ feature is disabled on the Cisco Nexus device. You can enable the TACACS+ feature to access the configuration and verification commands for authentication.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>switch(config)# feature tacacs+</td>
<td>Enables TACACS+.</td>
</tr>
<tr>
<td>switch(config)# exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>(Optional) switch# copy running-config</td>
<td>Copies the running configuration to the startup</td>
</tr>
<tr>
<td>startup-config</td>
<td>configuration.</td>
</tr>
</tbody>
</table>

Configuring TACACS+ Server Hosts

To access a remote TACACS+ server, you must configure the IPv4 address or the hostname for the TACACS+ server on the Cisco Nexus device. All TACACS+ server hosts are added to the default TACACS+ server group. You can configure up to 64 TACACS+ servers.

If a preshared key is not configured for a configured TACACS+ server, a warning message is issued if a global key is not configured. If a TACACS+ server key is not configured, the global key (if configured) is used for that server.

Before you configure TACACS+ server hosts, you should do the following:

• Enable TACACS+.
• Obtain the IPv4 addresses or the hostnames for the remote TACACS+ servers.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>switch(config)# exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>(Optional) switch# show tacacs-server</td>
<td>Displays the TACACS+ server configuration.</td>
</tr>
<tr>
<td>(Optional) switch# copy running-config</td>
<td>Copies the running configuration to the startup</td>
</tr>
<tr>
<td>startup-config</td>
<td>configuration.</td>
</tr>
</tbody>
</table>
Configuring TACACS+ Global Preshared Keys

You can configure preshared keys at the global level for all servers used by the Cisco Nexus device. A preshared key is a shared secret text string between the Cisco Nexus device and the TACACS+ server hosts.

Before you configure preshared keys, you should do the following:

- Enable TACACS+.
- Obtain the preshared key values for the remote TACACS+ servers.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# tacacs-server key [0</td>
<td>7] key-value</td>
</tr>
<tr>
<td>Step 3</td>
<td>switch(config)# exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) switch# show tacacs-server</td>
<td>Displays the TACACS+ server configuration.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td>The preshared keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted preshared keys.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Example

The following example shows how to configure global preshared keys:

```bash
switch# configure terminal
switch(config)# tacacs-server key 0 QsEfThUKo
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```
Configuring TACACS+ Server Preshared Keys

You can configure preshared keys for a TACACS+ server. A preshared key is a shared secret text string between the Cisco Nexus device and the TACACS+ server host.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) switch# show tacacs-server</td>
<td>Displays the TACACS+ server configuration. <strong>Note</strong>: The preshared keys are saved in encrypted form in the running configuration. Use the <code>show running-config</code> command to display the encrypted preshared keys.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to configure the TACACS+ preshared keys:

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

Configuring TACACS+ Server Groups

You can specify one or more remote AAA servers to authenticate users using server groups. All members of a group must belong to the TACACS+ protocol. The servers are tried in the same order in which you configure them.

You can configure these server groups at any time but they only take effect when you apply them to an AAA service.

**Before you begin**

You must use the `feature tacacs+` command to enable TACACS+ before you configure TACACS+.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
## Configuring TACACS+ Server Groups

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creates a TACACS+ server group and enters the TACACS+ server group configuration mode for that group.</td>
<td>switch(config)# aaa group server tacacs+ group-name</td>
</tr>
<tr>
<td>Configures the monitoring dead time. The default is 0 minutes. The range is from 0 through 1440.</td>
<td>(Optional) switch(config-tacacs+)# <strong>deadtime minutes</strong></td>
</tr>
<tr>
<td>Assigns a source interface for a specific TACACS+ server group.</td>
<td>(Optional) switch(config-tacacs+)# <strong>source-interface interface</strong></td>
</tr>
<tr>
<td>Exits configuration mode.</td>
<td>switch(config-tacacs+)# <strong>exit</strong></td>
</tr>
<tr>
<td>Displays the TACACS+ server group configuration.</td>
<td>(Optional) switch(config)# <strong>show tacacs-server groups</strong></td>
</tr>
<tr>
<td>Copies the running configuration to the startup configuration.</td>
<td>(Optional) switch(config)# <strong>copy running-config startup-config</strong></td>
</tr>
</tbody>
</table>

### Example

The following example shows how to configure a TACACS+ server group:

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config)# server 10.10.2.2
switch(config-tacacs+)# deadtime 30
switch(config-tacacs+)# exit
switch(config)# show tacacs-server groups
switch(config)# copy running-config startup-config
```
Configuring the Global Source Interface for TACACS+ Server Groups

You can configure a global source interface for TACACS+ server groups to use when accessing TACACS+ servers. You can also configure a different source interface for a specific TACACS+ server group.

### 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> ip tacacs source-interface</td>
<td>Configures the global source interface for all TACACS+ server groups</td>
</tr>
<tr>
<td>interface interface</td>
<td>configured on the device. The source interface can be the management</td>
</tr>
<tr>
<td>Example:</td>
<td>or the VLAN interface.</td>
</tr>
<tr>
<td>switch(config)# ip tacacs source-</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>interface mgmt 0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Displays the TACACS+ server configuration information.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# exit</td>
<td></td>
</tr>
<tr>
<td>switch#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) show tacacs-server</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# show tacacs-server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) copy running-config</td>
<td></td>
</tr>
<tr>
<td>config startup-config</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# copy running-config</td>
<td></td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Specifying a TACACS+ Server at Login

You can configure the switch to allow the user to specify which TACACS+ server to send the authenticate request by enabling the directed-request option. By default, a Cisco Nexus device forwards an authentication request based on the default AAA authentication method. If you enable this option, the user can log in as `username@hostname`, where `hostname` is the name of a configured RADIUS server.

**Note**: User specified logins are only supported for Telnet sessions.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> switch(config)#</td>
<td>Allows users to specify a TACACS+ server to send the authentication</td>
</tr>
<tr>
<td>tacacs-server directed-request</td>
<td>request when logging in. The default is disabled.</td>
</tr>
</tbody>
</table>
### Configuring the Global TACACS+ Timeout Interval

You can set a global timeout interval that the Cisco Nexus device waits for responses from all TACACS+ servers before declaring a timeout failure. The timeout interval determines how long the switch waits for responses from TACACS+ servers before declaring a timeout failure.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> switch(config)# tacacs-server timeout seconds</td>
<td>Specifies the timeout interval for TACACS+ servers. The default timeout interval is 5 seconds and the range is from 1 to 60 seconds.</td>
</tr>
<tr>
<td><strong>Step 3</strong> switch(config)# exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) switch# show tacacs-server</td>
<td>Displays the TACACS+ server configuration.</td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

### Configuring the Timeout Interval for a Server

You can set a timeout interval that the Cisco Nexus device waits for responses from a TACACS+ server before declaring a timeout failure. The timeout interval determines how long the switch waits for responses from a TACACS+ server before declaring a timeout failure.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> switch(config)# exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) switch# show tacacs-server</td>
<td>Displays the TACACS+ server configuration.</td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>
Configuring TCP Ports

You can configure another TCP port for the TACACS+ servers if there are conflicts with another application. By default, the Cisco Nexus device uses port 49 for all TACACS+ requests.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) switch# show tacacs-server</td>
<td>Displays the TACACS+ server configuration.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup</td>
</tr>
</tbody>
</table>

Example

The following example shows how to configure TCP ports:

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 port 2
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

Configuring Periodic TACACS+ Server Monitoring

You can monitor the availability of TACACS+ servers. These parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval in which a TACACS+ server receives no requests before the Cisco Nexus device sends out a test packet. You can configure this option to test servers periodically, or you can run a one-time only test.

Note

To protect network security, we recommend that you use a username that is not the same as an existing username in the TACACS+ database.

The test idle timer specifies the interval in which a TACACS+ server receives no requests before the Cisco Nexus device sends out a test packet.

Note

The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.
### Configuring TACACS+

#### Configuring the Dead-Time Interval

You can configure the dead-time interval for all TACACS+ servers. The dead-time interval specifies the time that the Cisco Nexus device waits, after declaring a TACACS+ server is dead, before sending out a test packet to determine if the server is now alive.

##### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>switch(config)# tacacs-server dead-time minutes</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switch(config)# exit</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) switch# show tacacs-server</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>

##### Example

The following example shows how to configure periodic TACACS+ server monitoring:

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3
switch(config)# tacacs-server dead-time 5
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

#### Configuring the Dead-Time Interval

When the dead-time interval is 0 minutes, TACACS+ servers are not marked as dead even if they are not responding. You can configure the dead-time interval per group.

##### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>switch(config)# tacacs-server deadtime minutes</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switch(config)# exit</td>
</tr>
</tbody>
</table>
### Configuring TACACS+

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4 (Optional) switch# show tacacs-server</td>
<td>Displays the TACACS+ server configuration.</td>
</tr>
<tr>
<td>Step 5 (Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

### Configuring ASCII Authentication

You can enable ASCII authentication on the TACACS+ server.

**Before you begin**

Enable TACACS+.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2 aaa authentication login ascii-authentication</td>
<td>Enables ASCII authentication. The default is disabled.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# aaa authentication login</td>
<td></td>
</tr>
<tr>
<td>ascii-authentication</td>
<td></td>
</tr>
<tr>
<td>Step 3 exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# exit</td>
<td></td>
</tr>
<tr>
<td>switch#</td>
<td></td>
</tr>
<tr>
<td>Step 4 (Optional) show tacacs-server</td>
<td>Displays the TACACS+ server configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# show tacacs-server</td>
<td></td>
</tr>
<tr>
<td>Step 5 (Optional) copy running-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Manually Monitoring TACACS+ Servers or Groups

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>switch# test aaa server tacacs+ {ipv4-address</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>switch# test aaa group group-name username password</td>
</tr>
</tbody>
</table>

#### Example

The following example shows how to manually issue a test message:

```plaintext
switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH
switch# test aaa group TacGroup user2 As3He3CI
```

### Disabling TACACS+

You can disable TACACS+.

⚠️ **Caution**

When you disable TACACS+, all related configurations are automatically discarded.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>switch(config)# no feature tacacs+</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switch(config)# exit</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>

### Displaying TACACS+ Statistics

To display the statistics, the switch maintains for TACACS+ activity, perform this task:

#### Example

For detailed information about the fields in the output from this command, see the Command Reference for your Nexus switch.
Verifying the TACACS+ Configuration

To display TACACS+ information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show tacacs+ [status</td>
<td>pending</td>
</tr>
<tr>
<td>show running-config tacacs [all]</td>
<td>Displays the TACACS+ configuration in the running configuration.</td>
</tr>
<tr>
<td>show startup-config tacacs</td>
<td>Displays the TACACS+ configuration in the startup configuration.</td>
</tr>
<tr>
<td>show tacacs-serve [host-name</td>
<td>ipv4-address</td>
</tr>
</tbody>
</table>

Configuration Examples for TACACS+

This example shows how to configure TACACS+:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# tacacs-server key 7 "ToIkLhPpG"
switch(config)# tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
switch(config-tacacs+)# use-vrf management
```

This example shows how to enable tacacs+ and how to configure the tacacs+ server preshared keys to specify remote AAA servers to authenticate server group TacServer1:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# tacacs-server key 7 "ikvhw10"
switch(config)# tacacs-server host 1.1.1.1
switch(config)# tacacs-server host 1.1.1.2
switch(config)# aaa group server tacacs+ TacServer1
switch(config-tacacs+)# server 1.1.1.1
switch(config-tacacs+)# server 1.1.1.2
```
CHAPTER 6

Configuring SSH and Telnet

This chapter contains the following sections:

• Information About SSH and Telnet, on page 63
• Guidelines and Limitations for SSH, on page 64
• Default Settings for SSH, on page 64
• Configuring SSH, on page 65
• Configuration Examples for SSH, on page 69
• Configuring Telnet, on page 71
• Verifying the SSH and Telnet Configuration, on page 72

Information About SSH and Telnet

SSH Server

The Secure Shell Protocol (SSH) server feature enables an SSH client to make a secure, encrypted connection to a Cisco Nexus device. SSH uses strong encryption for authentication. The SSH server in the Cisco Nexus device switch interoperates with publicly and commercially available SSH clients.

The user authentication mechanisms supported for SSH are RADIUS, TACACS+, and the use of locally stored user names and passwords.

SSH Client

The SSH client feature is an application running over the SSH protocol to provide device authentication and encryption. The SSH client enables a switch to make a secure, encrypted connection to another Cisco Nexus device or to any other device running an SSH server. This connection provides an outbound connection that is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

The SSH client in the Cisco Nexus device works with publicly and commercially available SSH servers.

SSH Server Keys

SSH requires server keys for secure communications to the Cisco Nexus device. You can use SSH keys for the following SSH options:
SSH version 2 using Rivest, Shamir, and Adelman (RSA) public-key cryptography

SSH version 2 using the Digital System Algorithm (DSA)

Be sure to have an SSH server key-pair with the appropriate version before enabling the SSH service. You can generate the SSH server key-pair according to the SSH client version used. The SSH service accepts three types of key-pairs for use by SSH version 2:

- The dsa option generates the DSA key-pair for the SSH version 2 protocol.
- The rsa option generates the RSA key-pair for the SSH version 2 protocol.

By default, the Cisco Nexus device generates an RSA key using 1024 bits.

SSH supports the following public key formats:

- OpenSSH
- IETF Secure Shell (SECSH)

---

Caution

If you delete all of the SSH keys, you cannot start the SSH services.

---

**Telnet Server**

The Telnet protocol enables TCP/IP connections to a host. Telnet allows a user at one site to establish a TCP connection to a login server at another site, and then passes the keystrokes from one system to the other. Telnet can accept either an IP address or a domain name as the remote system address.

The Telnet server is enabled by default on the Cisco Nexus device.

**Guidelines and Limitations for SSH**

SSH has the following configuration guidelines and limitations:

- The Cisco Nexus device supports only SSH version 2 (SSHv2).
- The SSH public and private keys imported into user accounts that are remotely authenticated through a AAA protocol (such as RADIUS or TACACS+) for the purpose of SSH passwordless file copy will not persist when the Cisco Nexus device is reloaded.

**Default Settings for SSH**

The following table lists the default settings for SSH parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH server</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Generating SSH Server Keys

You can generate an SSH server key based on your security requirements. The default SSH server key is an RSA key that is generated using 1024 bits.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>switch(config)# ssh key {dsa [force]</td>
<td>rsa [bits [force]]}</td>
</tr>
<tr>
<td>3</td>
<td>switch(config)# exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>(Optional) switch# show ssh key</td>
<td>Displays the SSH server keys.</td>
</tr>
<tr>
<td>5</td>
<td>(Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Example

The following example shows how to generate an SSH server key:

```
switch# configure terminal
switch(config)# ssh key rsa 2048
switch(config)# exit
switch# show ssh key
switch# copy running-config startup-config
```
Specifying the SSH Public Keys for User Accounts

You can configure an SSH public key to log in using an SSH client without being prompted for a password. You can specify the SSH public key in one of three different formats:

- Open SSH format
- IETF SECSH format
- Public Key Certificate in PEM format

Specifying the SSH Public Keys in Open SSH Format

You can specify the SSH public keys in SSH format for user accounts.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# username username sshkey ssh-key</td>
<td>Configures the SSH public key in SSH format.</td>
</tr>
<tr>
<td>Step 3</td>
<td>switch(config)# exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) switch# show user-account</td>
<td>Displays the user account configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to specify an SSH public key in open SSH format:

```
switch# configure terminal
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEwqUeyzCFTPO5B8tRkedn56BEy2k92zdpqG6aq3L2wZvFzC7FExzAAz5p9AS8dDgBAjJSKgs7UnxhGySr3EILv+DQBaDQH6zr2t0KRv+2Da8xJD4ZXiaccWkglS1DQUNZ300xstQeYzUtqxlbvm5Ninn0McNinn0Mc=
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

**Note**

The `username` command in the example above is a single line that has been broken for legibility.

Specifying the SSH Public Keys in IETF SECSH Format

You can specify the SSH public keys in IETF SECSH format for user accounts.
## Specifying the SSH Public Keys in PEM-Formatted Public Key Certificate Form

You can specify the SSH public keys in PEM-formatted Public Key Certificate form for user accounts.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> switch# copy server-file bootflash: filename</td>
<td>Downloads the file that contains the SSH key in PEM-formatted Public Key Certificate form from a server. The server can be FTP, SCP, SFTP, or TFTP.</td>
</tr>
<tr>
<td><strong>Step 2</strong> switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> switch(config)# username username sshkey file filename</td>
<td>Configures the SSH public key in PEM-formatted Public Key Certificate form.</td>
</tr>
<tr>
<td><strong>Step 4</strong> switch(config)# exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td>(Optional) <strong>Step 5</strong> switch# show user-account</td>
<td>Displays the user account configuration.</td>
</tr>
<tr>
<td>(Optional) <strong>Step 6</strong> switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

### Example

The following example shows how to specify the SSH public key in the PEM-formatted Public Key Certificate format:

```plaintext
switch#copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub
switch# configure terminal
switch(config)# username User1 sshkey file bootflash:secsh_file.pub
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```
Example

The following example shows how to specify the SSH public keys in PEM-formatted public key certificate form:

switch# copy tftp://10.10.1.1/cert.pem bootflash:cert.pem
switch# configure terminal
switch# show user-account
switch# copy running-config startup-config

Starting SSH Sessions to Remote Devices

You can start SSH sessions to connect to remote devices from your Cisco Nexus device.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>switch# ssh [hostname] [username@hostname] [vrf vrf-name]</code></td>
</tr>
</tbody>
</table>

Clearing SSH Hosts

When you download a file from a server using SCP or SFTP, you establish a trusted SSH relationship with that server.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>switch# clear ssh hosts</code></td>
</tr>
</tbody>
</table>

Disabling the SSH Server

By default, the SSH server is enabled on the Cisco Nexus device.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>switch# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>switch(config)# [no] feature ssh</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>switch(config)# exit</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) <code>switch# show ssh server</code></td>
</tr>
</tbody>
</table>
Deleting SSH Server Keys

You can delete SSH server keys after you disable the SSH server.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 switch(config)# no feature ssh</td>
<td>Disables the SSH server.</td>
</tr>
<tr>
<td>Step 3 switch(config)# no ssh key [dsa</td>
<td>rsa]</td>
</tr>
<tr>
<td>Step 4 switch(config)# exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td>Step 5 (Optional) switch# show ssh key</td>
<td>Displays the SSH server configuration.</td>
</tr>
<tr>
<td>Step 6 (Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Clearing SSH Sessions

You can clear SSH sessions from the Cisco Nexus device.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 switch# show users</td>
<td>Displays user session information.</td>
</tr>
<tr>
<td>Step 2 switch# clear line vty-line</td>
<td>Clears a user SSH session.</td>
</tr>
</tbody>
</table>

Configuration Examples for SSH

The following example shows how to configure SSH:
### Procedure

**Step 1** Generate an SSH server key.

```
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
```

**Step 2** Enable the SSH server.

```
switch# configure terminal
switch(config)# feature ssh
```

**Note** This step should not be required because the SSH server is enabled by default.

**Step 3** Display the SSH server key.

```
switch(config)# show ssh key
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYzCfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZ/cTFEzaAA2p9AS86dgBAjsKgs7UxnhGySr8ZELv+DQBsdQ86rzZt0KR+2Da8hJD4ZXIeccWk0gS1DQUNZ300xstQeYZUtqnx1bvm5/
Ninn0Mc=
```

```
bitcount:1024
fingerprint:
**************************************
could not retrieve dsa key information
**************************************
```

**Step 4** Specify the SSH public key in Open SSH format.

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAA2p9AS86dgBAjsKgs7UxnhGySr8ZELv+DQBsdQ86rzZt0KR+2Da8hJD4Z
XlIeccWk0gS1DQUNZ300xstQeYZUtqnx1bvm5Ninn0McNinn0Mc=
```

**Step 5** Save the configuration.

```
switch(config)# copy running-config startup-config
```
Configuring Telnet

Enabling the Telnet Server

By default, the Telnet server is enabled. You can disable the Telnet server on your Cisco Nexus device.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>switch(config)# [no] feature telnet</td>
<td>Enables/disables the Telnet server. The default is enabled.</td>
</tr>
</tbody>
</table>

Reenabling the Telnet Server

If the Telnet server on your Cisco Nexus device has been disabled, you can reenable it.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch(config)# [no] feature telnet</td>
<td>Reenables the Telnet server.</td>
</tr>
</tbody>
</table>

Starting Telnet Sessions to Remote Devices

Before you start a Telnet session to connect to remote devices, you should do the following:

- Obtain the hostname for the remote device and, if needed, obtain the username on the remote device.
- Enable the Telnet server on the Cisco Nexus device.
- Enable the Telnet server on the remote device.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch# telnet hostname</td>
<td>Creates a Telnet session to a remote device. The hostname argument can be an IPv4 address, an IPv6 address, or a device name.</td>
</tr>
</tbody>
</table>

Example

The following example shows how to start a Telnet session to connect to a remote device:

```
switch# telnet 10.10.1.1
```
Trying 10.10.1.1...
Connected to 10.10.1.1.
Escape character is '^]'.
switch login:

**Clearing Telnet Sessions**

You can clear Telnet sessions from the Cisco Nexus device.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> switch# show users</td>
<td>Displays user session information.</td>
</tr>
<tr>
<td><strong>Step 2</strong> switch# clear line vty-line</td>
<td>Clears a user Telnet session.</td>
</tr>
</tbody>
</table>

**Verifying the SSH and Telnet Configuration**

To display SSH and Telnet information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ssh key [dsa</td>
<td>rsa]</td>
</tr>
<tr>
<td>show running-config security [all]</td>
<td>Displays the SSH and user account configuration in the running configuration. The all keyword displays the default values for the SSH and user accounts.</td>
</tr>
<tr>
<td>show ssh server</td>
<td>Displays the SSH server configuration.</td>
</tr>
<tr>
<td>show user-account</td>
<td>Displays user account information.</td>
</tr>
</tbody>
</table>
CHAPTER 7

Configuring 802.1X

This chapter contains the following sections:

- Information About 802.1X, on page 73
- Licensing Requirements for 802.1X, on page 80
- Prerequisites for 802.1X, on page 80
- 802.1X Guidelines and Limitations, on page 80
- Default Settings for 802.1X, on page 81
- Configuring 802.1X, on page 82
- Verifying the 802.1X Configuration, on page 100
- Monitoring 802.1X, on page 101
- Configuration Example for 802.1X, on page 101
- Additional References for 802.1X, on page 101
- Feature History for 802.1X, on page 102

Information About 802.1X

802.1X defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a Cisco NX-OS device port.

Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

Device Roles

With 802.1X port-based authentication, the devices in the network have specific roles.

Figure 4: 802.1X Device Roles

This figure shows the device roles in 802.1X.
Device Roles

The specific roles are as follows:

**Supplicant**

The client device that requests access to the LAN and Cisco NX-OS device services and responds to requests from the Cisco NX-OS device. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating device.

**Note**

To resolve Windows XP network connectivity and Cisco 802.1X port-based authentication issues, read the Microsoft Knowledge Base article at this URL:

http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

**Authentication server**

The authentication server performs the actual authentication of the supplicant. The authentication server validates the identity of the supplicant and notifies the Cisco NX-OS device regarding whether the supplicant is authorized to access the LAN and Cisco NX-OS device services. Because the Cisco NX-OS device acts as the proxy, the authentication service is transparent to the supplicant. The Remote Authentication Dial-In User Service (RADIUS) security device with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server, version 3.0. RADIUS uses a supplicant-server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

**Authenticator**

The authenticator controls the physical access to the network based on the authentication status of the supplicant. The authenticator acts as an intermediary (proxy) between the supplicant and the authentication server, requesting identity information from the supplicant, verifying the requested identity information with the authentication server, and relaying a response to the supplicant. The authenticator includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

When the authenticator receives EAPOL frames and relays them to the authentication server, the authenticator strips off the Ethernet header and encapsulates the remaining EAP frame in the RADIUS format. This encapsulation process does not modify or examine the EAP frames, and the authentication server must support EAP within the native frame format. When the authenticator receives frames from the authentication server, the authenticator removes the server’s frame header, leaving the EAP frame, which the authenticator then encapsulates for Ethernet and sends to the supplicant.

**Note**

The Cisco NX-OS device can only be an 802.1X authenticator.
Authentication Initiation and Message Exchange

Either the authenticator (Cisco NX-OS device) or the supplicant (client) can initiate authentication. If you enable authentication on a port, the authenticator must initiate authentication when it determines that the port link state transitions from down to up. The authenticator then sends an EAP-request/identity frame to the supplicant to request its identity (typically, the authenticator sends an initial identity/request frame followed by one or more requests for authentication information). When the supplicant receives the frame, it responds with an EAP-response/identity frame.

If the supplicant does not receive an EAP-request/identity frame from the authenticator during bootup, the supplicant can initiate authentication by sending an EAPOL-start frame, which prompts the authenticator to request the supplicant’s identity.

If 802.1X is not enabled or supported on the network access device, the Cisco NX-OS device drops any EAPOL frames from the supplicant. If the supplicant does not receive an EAP-request/identity frame after three attempts to start authentication, the supplicant transmits data as if the port is in the authorized state. A port in the authorized state means that the supplicant has been successfully authenticated.

When the supplicant supplies its identity, the authenticator begins its role as the intermediary, passing EAP frames between the supplicant and the authentication server until authentication succeeds or fails. If the authentication succeeds, the authenticator port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used.

Figure 5: Message Exchange

This figure shows a message exchange initiated by the supplicant using the One-Time-Password (OTP) authentication method with a RADIUS server. The OTP authentication device uses a secret pass-phrase to generate a sequence of one-time (single use) passwords.
The user’s secret pass-phrase never crosses the network at any time such as during authentication or during pass-phrase changes.

**Authenticator PAE Status for Interfaces**

When you enable 802.1X on an interface, the Cisco NX-OS software creates an authenticator port access entity (PAE) instance. An authenticator PAE is a protocol entity that supports authentication on the interface. When you disable 802.1X on the interface, the Cisco NX-OS software does not automatically clear the authenticator PAE instances. You can explicitly remove the authenticator PAE from the interface and then reapply it, as needed.

**Ports in Authorized and Unauthorized States**

The authenticator port state determines if the supplicant is granted access to the network. The port starts in the unauthorized state. In this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a supplicant is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the supplicant to flow normally.

If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the authenticator 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 protocol, 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.

Ports can have the following authorization states:

- **Force authorized**
  Disables 802.1X port-based authentication and transitions to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. This authorization state is the default.

- **Force unauthorized**
  Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The authenticator cannot provide authentication services to the client through the interface.

- **Auto**
  Enables 802.1X port-based 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 transitions from down to up or when an EAPOL-start frame is received from the supplicant. The authenticator requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each supplicant that attempts to access the network is uniquely identified by the authenticator by using the supplicant’s MAC address.

If the supplicant is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated supplicant 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 authenticator can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and the supplicant is not granted network access.

When a supplicant logs off, it sends an EAPOL-logoff message, which causes the authenticator port to transition to the unauthorized state.
If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

**MAC Authentication Bypass**

You can configure the Cisco NX-OS device to authorize a supplicant based on the supplicant MAC address by using the MAC authentication bypass feature. For example, you can enable this feature on interfaces configured for 802.1X that are connected to devices such as printers.

If 802.1X authentication times out while waiting for an EAPOL response from the supplicant, the Cisco NX-OS device tries to authorize the client by using MAC authentication bypass.

When you enable the MAC authentication bypass feature on an interface, the Cisco NX-OS device uses the MAC address as the supplicant identity. The authentication server has a database of supplicant MAC addresses that are allowed network access. After detecting a client on the interface, the Cisco NX-OS device waits for an Ethernet packet from the client. The Cisco NX-OS device sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the Cisco NX-OS device grants the client access to the network. If authorization fails, the Cisco NX-OS device assigns the port to the guest VLAN if one is configured.

If an EAPOL packet is detected on the interface during the lifetime of the link, the Cisco NX-OS device 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 Cisco NX-OS device already authorized an interface by using MAC authentication bypass and detects an 802.1X supplicant, the Cisco NX-OS device does not unauthorize the client connected to the interface. When reauthentication occurs, the Cisco NX-OS device uses 802.1X authentication as the preferred reauthentication process if the previous session ended because the Termination-Action RADIUS attribute value is DEFAULT.

Clients that were authorized with MAC authentication bypass can be reauthenticated. The reauthentication process is the same as that for clients that were authenticated with 802.1X. During reauthentication, the port remains in the previously assigned VLAN. If reauthentication is successful, the switch keeps the port in the same VLAN. If reauthentication fails, the switch assigns the port to the guest VLAN, if one is configured.

If reauthentication 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 reauthentication. If MAC authentication bypass is enabled and the 802.1X authentication times out, the switch uses the MAC authentication bypass feature to initiate reauthorization. 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 following features:

- **802.1X authentication**—You can enable MAC authentication bypass only if 802.1X authentication is enabled on the port.
- **Port security**—You can configure 802.1X authentication and port security on the same Layer 2 ports.
- **Network admission control (NAC) Layer 2 IP validation**—This feature takes effect after an 802.1X port is authenticated with MAC authentication bypass, including hosts in the exception list.
802.1X and Port Security

You can configure port security and 802.1X on the same interfaces. Port security secures the MAC addresses that 802.1X authenticates. 802.1X processes packets before port security processes them, so when you enable both on an interface, 802.1X is already preventing inbound traffic on the interface from unknown MAC addresses.

When you enable 802.1X and port security on the same interface, port security continues to learn MAC addresses by the sticky or dynamic method, as configured. Additionally, depending on whether you enable 802.1X in single-host mode or multiple-host mode, one of the following occurs:

**Single host mode**
- Port security learns the MAC address of the authenticated host.

**Multiple host mode**
- Port security drops any MAC addresses learned for this interface by the dynamic method and learns the MAC address of the first host authenticated by 802.1X.

If a MAC address that 802.1X passes to port security would violate the applicable maximum number of secure MAC addresses, the device sends an authentication failure message to the host.

The device treats MAC addresses authenticated by 802.1X as though they were learned by the dynamic method, even if port security previously learned the address by the sticky or static methods. If you attempt to delete a secure MAC address that has been authenticated by 802.1X, the address remains secure.

If the MAC address of an authenticated host is secured by the sticky or static method, the device treats the address as if it were learned by the dynamic method, and you cannot delete the MAC address manually.

Port security integrates with 802.1X to reauthenticate hosts when the authenticated and secure MAC address of the host reaches its port security age limit. The device behaves differently depending upon the type of aging, as follows:

**Absolute**
- Port security notifies 802.1X and the device attempts to reauthenticate the host. The result of reauthentication determines whether the address remains secure. If reauthentication succeeds, the device restarts the aging timer on the secure address; otherwise, the device drops the address from the list of secure addresses for the interface.

**Inactivity**
- Port security drops the secure address from the list of secure addresses for the interface and notifies 802.1X. The device attempts to reauthenticate the host. If reauthentication succeeds, port security secures the address again.

Dynamic VLAN Assignment based on MAC-Based Authentication (MAB)

The Cisco Nexus 5000 and 6000 series switches supports dynamic VLAN assignment. After the 802.1x authentication or MAB is completed; before bringing up the port, you may want to (as part of authorization) allow the peer/host to be placed into a particular VLAN based as a result of the authentication. The RADIUS server typically indicates the desired VLAN by including tunnel attributes within the Access-Accept message. This procedure of getting the VLAN an binding it to the port constitutes to Dynamic VLAN assignment.
VLAN Assignment from RADIUS

After authentication is completed either through dot1x or MAB, the response from the RADIUS server can have dynamic VLAN information, which can be assigned to a port. This information is present in response from RADIUS server in Accept-Access message in the form of tunnel attributes. For use in VLAN assignment, the following tunnel attributes are sent:

- Tunnel-type=VLAN(13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

All the three parameters must be received for configuring access VLAN.

Single Host and Multiple Hosts Support

The 802.1X feature can restrict traffic on a port to only one endpoint device (single-host mode) or allow traffic from multiple endpoint devices on a port (multi-host mode).

Single-host mode allows traffic from only one endpoint device on the 802.1X port. Once the endpoint device is authenticated, the Cisco NX-OS device puts the port in the authorized state. When the endpoint device leaves the port, the Cisco NX-OS device puts the port back into the unauthorized state. A security violation in 802.1X is defined as a detection of frames sourced from any MAC address other than the single MAC address authorized as a result of successful authentication. In this case, the interface on which this security association violation is detected (EAPOL frame from the other MAC address) will be disabled. Single host mode is applicable only for host-to-switch topology and when a single host is connected to the Layer 2 (Ethernet access port) or Layer 3 port (routed port) of the Cisco NX-OS device.

Only the first host has to be authenticated on the 802.1X port configured with multiple host mode. The port is moved to the authorized state after the successful authorization of the first host. Subsequent hosts are not required to be authorized to gain network access once the port is in the authorized state. If the port becomes unauthorized when reauthentication fails or an EAPOL logoff message is received, all attached hosts are denied access to the network. The capability of the interface to shut down upon security association violation is disabled in multiple host mode. This mode is applicable for both switch-to-switch and host-to-switch topologies.

Supported Topologies

The 802.1X port-based authentication is supported in two topologies:

- Point-to-point
- Wireless LAN

In a point-to-point configuration, only one supplicant (client) can connect to the 802.1X-enabled authenticator (Cisco NX-OS device) port. The authenticator detects the supplicant when the port link state changes to the up state. If a supplicant leaves or is replaced with another supplicant, the authenticator changes the port link state to down, and the port returns to the unauthorized state.
Licensing Requirements for 802.1X

The following table shows the licensing requirements for this feature:

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>802.1X requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you.</td>
</tr>
</tbody>
</table>

Prerequisites for 802.1X

802.1X Guidelines and Limitations

802.1X port-based authentication has the following configuration guidelines and limitations:

- The Cisco NX-OS software supports 802.1X authentication only on physical ports.
- The Cisco NX-OS software does not support 802.1X authentication on port channels or subinterfaces.
- When you enable 802.1X authentication, supplicants are authenticated before any other Layer 2 or Layer 3 features are enabled on an Ethernet interface.
- The Cisco NX-OS software supports 802.1X authentication only on Ethernet interfaces that are in a port channel, a trunk, or an access port.
- The Cisco NX-OS software does not support single host mode on trunk interfaces or member interfaces in a port channel.
- The Cisco NX-OS software does not support MAC address authentication bypass on trunk interfaces.
- The Cisco NX-OS software does not support MAC address authentication bypass on a port channel.
The Cisco NX-OS software does not support Dot1X on vPC ports and MCT.

The Cisco NX-OS software does not support the following 802.1X protocol enhancements:
- One-to-many logical VLAN name to ID mapping
- Web authorization
- Dynamic domain bridge assignment
- IP telephony

### Default Settings for 802.1X

This table lists the default settings for 802.1X parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X feature</td>
<td>Disabled</td>
</tr>
<tr>
<td>AAA 802.1X authentication method</td>
<td>Not configured</td>
</tr>
<tr>
<td>Per-interface 802.1X protocol enable state</td>
<td>Disabled (force-authorized)</td>
</tr>
<tr>
<td>Per-interface 802.1X protocol enable state</td>
<td></td>
</tr>
<tr>
<td>Note: The port transmits and receives normal</td>
<td></td>
</tr>
<tr>
<td>traffic without 802.1X-based authentication</td>
<td></td>
</tr>
<tr>
<td>of the supplicant.</td>
<td></td>
</tr>
<tr>
<td>Periodic reauthentication</td>
<td>Disabled</td>
</tr>
<tr>
<td>Number of seconds between reauthentication</td>
<td>3600 seconds</td>
</tr>
<tr>
<td>attempts</td>
<td></td>
</tr>
<tr>
<td>Quiet timeout period</td>
<td>60 seconds (number of seconds that the Cisco NX-OS device remains in the</td>
</tr>
<tr>
<td></td>
<td>quiet state following a failed authentication exchange with the</td>
</tr>
<tr>
<td></td>
<td>supplicant)</td>
</tr>
<tr>
<td>Retransmission timeout period</td>
<td>30 seconds (number of seconds that the Cisco NX-OS device should wait</td>
</tr>
<tr>
<td></td>
<td>for a response to an EAP request/identity frame from the supplicant</td>
</tr>
<tr>
<td></td>
<td>before retransmitting the request)</td>
</tr>
<tr>
<td>Maximum retransmission number</td>
<td>2 times (number of times that the Cisco NX-OS device will send an</td>
</tr>
<tr>
<td></td>
<td>EAP-request/identity frame before restarting the authentication</td>
</tr>
<tr>
<td></td>
<td>process)</td>
</tr>
<tr>
<td>Host mode</td>
<td>Single host</td>
</tr>
<tr>
<td>Supplicant timeout period</td>
<td>30 seconds (when relaying a request from the authentication server to</td>
</tr>
<tr>
<td></td>
<td>the supplicant, the amount of time that the Cisco NX-OS device waits</td>
</tr>
<tr>
<td></td>
<td>for a response before retransmitting the request to the supplicant)</td>
</tr>
</tbody>
</table>
### Configuring 802.1X

This section describes how to configure the 802.1X feature.

### Process for Configuring 802.1X

This section describes the process for configuring 802.1X.

#### Procedure

1. **Step 1** Enable the 802.1X feature.
2. **Step 2** Configure the connection to the remote RADIUS server.
3. **Step 3** Enable 802.1X feature on the Ethernet interfaces.

### Enabling the 802.1X Feature

You must enable the 802.1X feature on the Cisco NX-OS device before authenticating any supplicant devices.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>feature dot1x</code></td>
<td>Enables the 802.1X feature. The default is disabled.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# feature dot1x</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>exit</code></td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# exit</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch#</code></td>
<td></td>
</tr>
</tbody>
</table>

#### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication server timeout period</td>
<td>30 seconds (when relaying a response from the supplicant to the authentication server, the amount of time that the Cisco NX-OS device waits for a reply before retransmitting the response to the server)</td>
</tr>
</tbody>
</table>
### Configuring AAA Authentication Methods for 802.1X

You can use remote RADIUS servers for 802.1X authentication. You must configure RADIUS servers and RADIUS server groups and specify the default AAA authentication method before the Cisco NX-OS device can perform 802.1X authentication.

#### Before you begin

Obtain the names or addresses for the remote RADIUS server groups.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> aaa authentication dot1x default group group-list</td>
<td>Specifies the RADIUS server groups to use for 802.1X authentication. The <em>group-list</em> argument consists of a space-delimited list of group names. The group names are the following:</td>
</tr>
<tr>
<td>Example: switch(config)# aaa authentication dot1x default group rad2</td>
<td>• radius—Uses the global pool of RADIUS servers for authentication.</td>
</tr>
<tr>
<td></td>
<td>• named-group—Uses the global pool of RADIUS servers for authentication.</td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Example: switch(config)# exit switch#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) show radius-server</td>
<td>Displays the RADIUS server configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch# show radius-server</td>
<td>Displays the RADIUS server group configuration.</td>
</tr>
</tbody>
</table>

**Step 5** (Optional)  
**show radius-server group [group-name]**

**Example:**  
switch# show radius-server group rad2

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Step 6** (Optional)  
**copy running-config startup-config**

**Example:**  
switch# copy running-config startup-config

---

### Controlling 802.1X Authentication on an Interface

You can control the 802.1X authentication performed on an interface. An interface can have the following 802.1X authentication states:

**Auto**  
Enables 802.1X authentication on the interface.

**Force-authorized**  
Disables 802.1X authentication on the interface and allows all traffic on the interface without authentication. This state is the default.

**Force-unauthorized**  
Disallows all traffic on the interface.

**Before you begin**  
Enable the 802.1X feature on the Cisco NX-OS device.

### Procedure

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

**Example:**  
switch# configure terminal  
switch(config)#

**Step 2**  
**interface ethernet slot/port**

**Example:**  
switch(config)# interface ethernet 2/1  
switch(config-if)#

**Step 3**  
**dot1x port-control {auto | force-authorized | forced-unauthorized}**

**Example:**  
switch(config-if)# dot1x port-control auto

Changes the 802.1X authentication state on the interface. The default is force-authorized.
### Configuring 802.1X Authentication on Member Ports

You can configure 802.1X authentication on the members of a port channel.

---

**Note**

You cannot configure 802.1X authentication on the port channel itself.

There are two ways to configure 802.1X authentication on member ports: 1) by configuring 802.1X on a member port and then adding the port to a port channel or 2) by creating a port channel, adding a port to the port channel, and then configuring 802.1X on the port. The following procedure provides instructions for the first method. To configure 802.1X using the second method, use these commands:

- `interface port-channel channel-number`
- `interface ethernet slot/port`
- `channel-group channel-number [force] [mode {on | active | passive}]`
- `dot1x port-control auto`

---

**Note**

For more information on the above commands, see the *Cisco NX-OS Interfaces Command Reference* for your platform.
Before you begin
Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>interface ethernet slot/port</code></td>
<td>Selects the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# interface ethernet 7/1</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-if)#</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>dot1x port-control auto</code></td>
<td>Changes the 802.1X authentication state on the interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-if)# dot1x port-control auto</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>[no] switchport</code></td>
<td>Configures the interface as a Layer 2 port or, if you use the no keyword, as a Layer 3 port.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-if)# switchport</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>dot1x host-mode multi-host</code></td>
<td>Enables multiple hosts mode for the interface. This command is required in order to add a port to a port channel.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-if)# dot1x host-mode multi-host</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>`channel-group channel-number [force] [mode {on</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-if)# channel-group 5 force</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>exit</code></td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Creating or Removing an Authenticator PAE on an Interface

You can create or remove the 802.1X authenticator port access entity (PAE) instance on an interface.

**Before you begin**

Enable the 802.1X feature.

**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><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
</tbody>
</table>
Enabling Periodic Reauthentication for an Interface

You can enable periodic 802.1X reauthentication on an interface and specify how often it occurs. If you do not specify a time period before enabling reauthentication, the number of seconds between reauthentication defaults to the global value.

---

**Note**
During the reauthentication process, the status of an already authenticated supplicant is not disrupted.

**Before you begin**
Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
configure terminal
Example:
switch# configure terminal
switch(config)# | Enters global configuration mode. |

---

Enabling Periodic Reauthentication for an Interface

You can enable periodic 802.1X reauthentication on an interface and specify how often it occurs. If you do not specify a time period before enabling reauthentication, the number of seconds between reauthentication defaults to the global value.

---

**Note**
During the reauthentication process, the status of an already authenticated supplicant is not disrupted.

**Before you begin**
Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2**
(Optional) show dot1x interface ethernet slot/port
Example:
switch# show dot1x interface ethernet 2/1 | Displays the 802.1X configuration on the interface. |

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3**
interface ethernet slot/port
Example:
switch(config)# interface ethernet 2/1
switch(config-if)# | Selects the interface to configure and enters interface configuration mode. |

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 4**
[no] dot1x pae authenticator
Example:
switch(config-if)# dot1x pae authenticator | Creates an authenticator PAE instance on the interface. Use the no form to remove the PAE instance from the interface. |

**Note**
If an authenticator PAE already exists on the interface the dot1x pae authentication command does not change the configuration on the interface.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 5**
(Optional) copy running-config startup-config
Example:
switch(config)# copy running-config startup-config | Copies the running configuration to the startup configuration. |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Selects the interface to configure and enters interface configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** | switch(config)# interface ethernet 2/1  
switch(config-if)# |
| **Step 3** | Enables periodic reauthentication of the supplicants connected to the interface. By default, periodic authentication is disabled. |
| **Example:** | switch(config-if)# dot1x re-authentication |
| **Step 4** | Sets the number of seconds between reauthentication attempts. The default is 3600 seconds. The range is from 1 to 65535. |
| **Example:** | switch(config-if)# dot1x timeout re-authperiod 3300 |
| **Note** | This command affects the behavior of the Cisco NX-OS device only if you enable periodic reauthentication on the interface. |
| **Step 5** | Exits configuration mode. |
| **Example:** | switch(config-if)# exit  
switch(config)# |
| **Step 6** | Displays all 802.1X feature status and configuration information. |
| **Example:** | switch(config)# show dot1x all |
| **Step 7** | Copies the running configuration to the startup configuration. |
| **Example:** | switch(config)# copy running-config startup-config |

---

### Manually Reauthenticating Supplicants

You can manually reauthenticate the supplicants for the entire Cisco NX-OS device or for an interface.

**Note**

During the reauthentication process, the status of an already authenticated supplicant is not disrupted.

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.
Manually Initializing 802.1X Authentication

You can manually initialize the authentication for all supplicants on a Cisco NX-OS device or for a specific interface.

Before you begin
Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Step 1</em></td>
<td></td>
</tr>
<tr>
<td><code>dot1x re-authenticate [interface slot/port]</code></td>
<td>Reauthenticates the supplicants on the Cisco NX-OS device or on an interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch# dot1x re-authenticate interface 2/1</code></td>
<td></td>
</tr>
</tbody>
</table>

Changing 802.1X Authentication Timers for an Interface

You can change the following 802.1X authentication timers on the Cisco NX-OS device interfaces:

**Quiet-period timer**
When the Cisco NX-OS device cannot authenticate the supplicant, the switch remains idle for a set period of time and then tries again. The quiet-period timer value determines the idle period. An authentication failure might occur because the supplicant provided an invalid password. You can provide a faster response time to the user by entering a smaller number than the default. The default is the value of the global quiet period timer. The range is from 1 to 65535 seconds.

**Rate-limit timer**
The rate-limit period throttles EAPOL-Start packets from supplicants that are sending too many EAPOL-Start packets. The authenticator ignores EAPOL-Start packets from supplicants that have successfully authenticated for the rate-limit period duration. The default value is 0 seconds and the authenticator processes all EAPOL-Start packets. The range is from 1 to 65535 seconds.
Switch-to-authentication-server retransmission timer for Layer 4 packets
The authentication server notifies the switch each time that it receives a Layer 4 packet. If the switch does not receive a notification after sending a packet, the Cisco NX-OS device waits a set period of time and then retransmits the packet. The default is 30 seconds. The range is from 1 to 65535 seconds.

Switch-to-suppliant retransmission timer for EAP response frames
The supplicant responds to the EAP-request/identity frame from the Cisco NX-OS device with an EAP-response/identity frame. If the Cisco NX-OS device does not receive this response, it waits a set period of time (known as the retransmission time) and then retransmits the frame. The default is 30 seconds. The range is from 1 to 65535 seconds.

Switch-to-suppliant retransmission timer for EAP request frames
The supplicant notifies the Cisco NX-OS device it that received the EAP request frame. If the authenticator does not receive this notification, it waits a set period of time and then retransmits the frame. The default is the value of the global retransmission period timer. The range is from 1 to 65535 seconds.

You should change the default values only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

Before you begin
Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>interface ethernet slot/port</td>
<td>Selects the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# interface ethernet 2/1</td>
<td></td>
</tr>
<tr>
<td>switch(config-if)</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Sets the number of seconds that the authenticator waits for a response to an EAP-request/identity frame from the supplicant before retransmitting the request. The default is the global number of seconds set for all interfaces. The range is from 1 to 65535 seconds.</td>
</tr>
<tr>
<td>(Optional) dot1x timeout quiet-period seconds</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-if)# dot1x timeout quiet-period 25</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Sets the number of seconds that the authenticator ignores EAPOL-Start packets from supplicants that have successfully authenticated. The default value is 0 seconds. The range is from 1 to 65535 seconds.</td>
</tr>
<tr>
<td>(Optional) dot1x timeout ratelimit-period seconds</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-if)# dot1x timeout ratelimit-period 10</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 5    | (Optional) dot1x timeout server-timeout seconds | Sets the number of seconds that the Cisco NX-OS device waits before retransmitting a packet to the authentication server. The default is 30 seconds. The range is from 1 to 65535 seconds. **Example:**
```
switch(config-if)# dot1x timeout server-timeout 60
```
| 6    | (Optional) dot1x timeout supp-timeout seconds | Sets the number of seconds that the Cisco NX-OS device waits for the supplicant to respond to an EAP request frame before the Cisco NX-OS device retransmits the frame. The default is 30 seconds. The range is from 1 to 65535 seconds. **Example:**
```
switch(config-if)# dot1x timeout supp-timeout 20
```
| 7    | (Optional) dot1x timeout tx-period seconds | Sets the number of seconds between the retransmission of EAP request frames when the supplicant does not send notification that it received the request. The default is the global number of seconds set for all interfaces. The range is from 1 to 65535 seconds. **Example:**
```
switch(config-if)# dot1x timeout tx-period 40
```
| 8    | exit | Exits configuration mode. **Example:**
```
switch(config)# exit
```
| 9    | (Optional) show dot1x all | Displays the 802.1X configuration. **Example:**
```
switch# show dot1x all
```
| 10   | (Optional) copy running-config startup-config | Copies the running configuration to the startup configuration. **Example:**
```
switch# copy running-config startup-config
```

## Enabling Single Host or Multiple Hosts Mode

You can enable single host or multiple hosts mode on an interface.

**Before you begin**
Enable the 802.1X feature on the Cisco NX-OS device.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface ethernet slot/port</td>
<td>Selects the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# interface ethernet 2/1</td>
<td></td>
</tr>
<tr>
<td>switch(config-if)</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dot1x host-mode {multi-host</td>
<td>single-host}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-if)# dot1x host-mode multi-host</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Make sure that the dot1x port-control interface configuration command is set to auto for the specified interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) show dot1x all</td>
<td>Displays all 802.1X feature status and configuration information.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# show dot1x all</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> (Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling MAC Authentication Bypass

You can enable MAC authentication bypass on an interface that has no supplicant connected.

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.

**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>
</tbody>
</table>
Disabling 802.1X Authentication on the Cisco NX-OS Device

You can disable 802.1X authentication on the Cisco NX-OS device. By default, the Cisco NX-OS software enables 802.1X authentication after you enable the 802.1X feature. However, when you disable the 802.1X feature, the configuration is removed from the Cisco NX-OS device. The Cisco NX-OS software allows you to disable 802.1X authentication without losing the 802.1X configuration.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

Note

When you disable 802.1X authentication, the port mode for all interfaces defaults to force-authorized regardless of the configured port mode. When you reenable 802.1X authentication, the Cisco NX-OS software restores the configured port mode on the interfaces.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> no dot1x system-auth-control</td>
<td>Disables 802.1X authentication on the Cisco NX-OS device. The default is enabled.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# no dot1x system-auth-control</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# exit</td>
<td></td>
</tr>
<tr>
<td>switch#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) show dot1x</td>
<td>Displays the 802.1X feature status.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# show dot1x</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Disabling the 802.1X Feature

You can disable the 802.1X feature on the Cisco NX-OS device.

When you disable 802.1X, all related configurations are automatically discarded. The Cisco NX-OS software creates an automatic checkpoint that you can use if you reenable 802.1X and want to recover the configuration. For more information, see the *Cisco NX-OS System Management Configuration Guide* for your platform.

### Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

### 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>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| `switch# configure terminal`  
`switch(config)#` | Enables 802.1X. |

**Step 2**  
**Example:**  
`switch(config)# no feature dot1x`  
Disables the 802.1X feature.  
**Caution** Disabling the 802.1X feature removes all 802.1X configuration.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Exits configuration mode.</td>
</tr>
</tbody>
</table>

**Step 3**  
**Example:**  
`switch(config)# exit`  

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| (Optional) `copy running-config startup-config`  
**Example:**  
`switch# copy running-config startup-config` | Copies the running configuration to the startup configuration. |

### Setting the Maximum Authenticator-to-Supplicant Frame Retransmission Retry Count for an Interface

You can set the maximum number of times that the Cisco NX-OS device retransmits authentication requests to the supplicant on an interface before the session times out. The default is 2 times and the range is from 1 to 10.

**Before you begin**  
Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `configure terminal`  
**Example:**  
`switch# configure terminal`  
`switch(config)#` | Enters global configuration mode. |

**Step 2**  
**Example:**  
`switch(config)# interface ethernet slot/port`  
Selects the interface to configure and enters interface configuration mode.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `dot1x max-req count`  
**Example:**  
`switch(config-if)# dot1x max-req 3` | Changes the maximum authorization request retry count. The default is 2 times and the range is from 1 to 10. |
Enabling RADIUS Accounting for 802.1X Authentication

You can enable RADIUS accounting for the 802.1X authentication activity.

Before you begin
Enable the 802.1X feature on the Cisco NX-OS device.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> dot1x radius-accounting</td>
<td>Enables RADIUS accounting for 802.1X. The default is disabled.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# dot1x radius-accounting</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# exit</td>
<td></td>
</tr>
<tr>
<td>switch#</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring AAA Accounting Methods for 802.1X

You can enable AAA accounting methods for the 802.1X feature.

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

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

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
|        | aaa accounting dot1x default group group-list | Configures AAA accounting for 802.1X. The default is disabled. The *group-list* argument consists of a space-delimited list of group names. The group names are the following:

- *radius*—For all configured RADIUS servers.
- *named-group*—Any configured RADIUS server group name. |

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>Exits configuration mode.</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>(Optional) show aaa accounting</td>
<td>Displays the AAA accounting configuration.</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>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to enable the 802.1x feature:

```
switch# configure terminal
switch(config)# aaa accounting dot1x default group radius
switch(config)# exit
```
### Setting the Maximum Reauthentication Retry Count on an Interface

You can set the maximum number of times that the Cisco NX-OS device retransmits reauthentication requests to the supplicant on an interface before the session times out. The default is 2 times and the range is from 1 to 10.

#### Before you begin
Enable the 802.1X feature on the Cisco NX-OS device.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `configure terminal` | Enters global configuration mode.  
*Example:*  
```
switch# configure terminal  
switch(config)#
``` |
| **Step 2** | `interface ethernet slot/port` | Selects the interface to configure and enters interface configuration mode.  
*Example:*  
```
switch(config)# interface ethernet 2/1  
switch(config-if)#
``` |
| **Step 3** | `dot1x max-reauth-req retry-count` | Changes the maximum reauthentication request retry count. The default is 2 times and the range is from 1 to 10.  
*Example:*  
```
switch(config-if)# dot1x max-reauth-req 3
``` |
| **Step 4** | `exit` | Exits interface configuration mode.  
*Example:*  
```
switch(config)# exit  
switch#
``` |
| **Step 5** | *(Optional)* `show dot1x all` | Displays all 802.1X feature status and configuration information.  
*Example:*  
```
switch# show dot1x all
``` |
| **Step 6** | *(Optional)* `copy running-config startup-config` |Copies the running configuration to the startup configuration.  
*Example:*  
```
switch(config)# copy running-config startup-config
``` |
Configuring Guest VLAN

If MAB is configured, and if there is an authentication failure due to MAB, then the guest VLAN (if available), will be assigned as access 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 global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface ethernet slot 1 port</td>
<td>Selects the interface to configure and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# interface ethernet 2/1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>dot1x guest-vlan guest-vlan</td>
<td>Specifies the guest VLAN to be assigned.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-if)# dot1x guest-vlan 5</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-if)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the 802.1X Configuration

To display 802.1X information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dot1x</td>
<td>Displays the 802.1X feature status.</td>
</tr>
<tr>
<td>show dot1x all [details</td>
<td>statistics</td>
</tr>
<tr>
<td>show dot1x interface ethernet slot/port [details</td>
<td>statistics</td>
</tr>
<tr>
<td>show running-config dot1x [all]</td>
<td>Displays the 802.1X feature configuration in the running configuration.</td>
</tr>
<tr>
<td>show startup-config dot1x</td>
<td>Displays the 802.1X feature configuration in the startup configuration.</td>
</tr>
</tbody>
</table>

For detailed information about the fields in the output from these commands, see the Cisco NX-OS Security Command Reference for your platform.
Monitoring 802.1X

You can display the statistics that the Cisco NX-OS device maintains for the 802.1X activity.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS 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><code>show dot1x all statistics</code></td>
<td>Displays the 802.1X statistics.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switch# show dot1x all statistics</code></td>
<td></td>
</tr>
</tbody>
</table>

Configuration Example for 802.1X

The following example shows how to configure 802.1X for an access port:

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae-authenticator
dot1x port-control auto
```

The following example shows how to configure 802.1X for a trunk port:

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae-authenticator
dot1x port-control auto
dot1x host-mode multi-host
```

### Note

Repeat the `dot1x pae authenticator` and `dot1x port-control auto` commands for all interfaces that require 802.1X authentication.

Additional References for 802.1X

This section includes additional information related to implementing 802.1X.
Feature History for 802.1X

Table 10: Feature History for 802.1X

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>6.0(2)N1(2)</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

To locate and download MIBs, go to the following URL:

CHAPTER 8

Configuring Cisco TrustSec

This chapter describes how to configure Cisco TrustSec on Cisco NX-OS devices.

This chapter includes the following sections:

- Information About Cisco TrustSec, on page 103
- Licensing Requirements for Cisco TrustSec, on page 112
- Prerequisites for Cisco TrustSec, on page 112
- Guidelines and Limitations for Cisco TrustSec, on page 112
- Default Settings for Cisco TrustSec Parameters, on page 113
- Configuring Cisco TrustSec, on page 113
- Verifying the Cisco TrustSec Configuration, on page 142
- Configuration Examples for Cisco TrustSec, on page 143
- Additional References for Cisco TrustSec, on page 146
- Feature History for Cisco TrustSec, on page 147

Information About Cisco TrustSec

This section provides information about Cisco TrustSec.

Cisco TrustSec Architecture

The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices. Cisco TrustSec also uses the device information acquired during authentication for classifying, or coloring, the packets as they enter the network. This packet classification is maintained by tagging packets on ingress to the Cisco TrustSec network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic.

Note

Ingress refers to entering the first Cisco TrustSec-capable device encountered by a packet on its path to the destination and egress refers to leaving the last Cisco TrustSec-capable device on the path.
This figure shows an example of a Cisco TrustSec cloud. In this example, several networking devices and an endpoint device are inside the Cisco TrustSec cloud. One endpoint device and one networking device are outside the cloud because they are not Cisco TrustSec-capable.

The Cisco TrustSec architecture consists of the following major components:

**Authentication**
- Verifies the identity of each device before allowing them to join the Cisco TrustSec network.

**Authorization**
- Decides the level of access to the Cisco TrustSec network resources for a device based on the authenticated identity of the device.

**Access control**
- Applies access policies on a per-packet basis using the source tags on each packet.

A Cisco TrustSec network has the following entities:

**Authenticators (AT)**
- Devices that are already part of a Cisco TrustSec network.

**Authorization server (AS)**
- Servers that may provide authentication information, authorization information, or both.

When the link first comes up, authorization occurs in which each side of the link obtains policies, such as SGT and ACLs, that apply to the link.

### Authentication

Cisco TrustSec authenticates a device before allowing it to join the network. Cisco TrustSec uses 802.1X authentication with Extensible Authentication Protocol Flexible Authentication through Secure Tunnel (EAP-FAST) as the Extensible Authentication Protocol (EAP) method to perform the authentication.

### Cisco TrustSec and Authentication

Cisco TrustSec uses EAP-FAST for authentication. EAP-FAST conversations allow other EAP method exchanges inside the EAP-FAST tunnel using chains, which allows administrators to use traditional user authentication methods.
authentication methods, such as Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2), while still having security provided by the EAP-FAST tunnel.

Figure 8: Cisco TrustSec Authentication

This figure shows the EAP-FAST tunnel and inner methods used in Cisco

Switch 1 (supplicant)  Switch 2 (authenticator)  AS

EAP-FAST in 802.1X  EAP-FAST in RADIUS

One-time provisioning  Device authentication

User authentication  EAP-FAST tunnel tear down

Policy acquisition  Policy acquisition (RADIUS)

Key establishment (SAP)  Ongoing key refresh (SAP)

Cisco TrustSec Enhancements to EAP-FAST

The implementation of EAP-FAST for Cisco TrustSec has the following enhancements:

Authenticate the authenticator

Securely determines the identity of the AT by requiring the AT to use its protected access credential (PAC) to derive the shared secret between itself and the authentication server. This feature also prevents you from configuring RADIUS shared secrets on the authentication server for every possible IP address that can be used by the AT.
Notify each peer of the identity of its neighbor

By the end of the authentication exchange, the authentication server has identified the supplicant and the AT. The authentication server conveys the identity of the AT, and whether the AT is Cisco TrustSec-capable, to the supplicant by using additional type-length-value parameters (TLVs) in the protected EAP-FAST termination. The authentication server also conveys the identity of the supplicant and whether the supplicant is Cisco TrustSec-capable to the AT by using RADIUS attributes in the Access-Accept message. Because each peer knows the identity of its neighbor, it can send additional RADIUS Access-Requests to the authentication server to acquire the policy to be applied on the link.

AT posture evaluation

The AT provides its posture information to the authentication server whenever it starts the authentication exchange with the authentication server on behalf of the supplicant.

802.1X Role Selection

In 802.1X, the AT must have IP connectivity with the authentication server because it has to relay the authentication exchange between the supplicant and the AT using RADIUS over UDP/IP. When an endpoint device, such as a PC, connects to a network, it is obvious that it should act as a supplicant. However, in the case of a Cisco TrustSec connection between two network devices, the 802.1X role of each network device might not be immediately apparent to the other network device.

Instead of requiring manual configuration of the AT and supplicant roles for the Cisco NX-OS devices, Cisco TrustSec runs a role-selection algorithm to automatically determine which Cisco NX-OS device acts as the AT and which device acts as the supplicant. The role-selection algorithm assigns the AT role to the device that has IP reachability to a RADIUS server. Both devices start both the AT and supplicant state machines. When a Cisco NX-OS device detects that its peer has access to a RADIUS server, it terminates its own AT state machine and assumes the role of the supplicant. If both Cisco NX-OS devices have access to a RADIUS server, the algorithm compares the MAC addresses used as the source for sending the EAP over LAN (EAPOL) packets. The Cisco NX-OS device that has the MAC address with the higher value becomes the AT and the other Cisco NX-OS device becomes the supplicant.

Cisco TrustSec Authentication Summary

By the end of the Cisco TrustSec authentication process, the authentication server has performed the following actions:

• Verified the identities of the supplicant and the AT
• Authenticated the user if the supplicant is an endpoint device

At the end of the Cisco TrustSec authentication process, the AT and the supplicant have the following information:

• Device ID of the peer
• Cisco TrustSec capability information of the peer
• Key used for the SA protocol

Device Identities

Cisco TrustSec does not use IP addresses or MAC addresses as device identities. Instead, assign a name (device ID) to each Cisco TrustSec-capable Cisco NX-OS device to identify it uniquely in the Cisco TrustSec network. This device ID is used for the following:

• Looking up authorization policy
Looking up passwords in the databases during authentication

**Device Credentials**

Cisco TrustSec supports password-based credentials. The authentication servers may use self-signed certificates instead. Cisco TrustSec authenticates the supplicants through passwords and uses MSCHAPv2 to provide mutual authentication even if the authentication server certificate is not verifiable.

The authentication server uses these credentials to mutually authenticate the supplicant during the EAP-FAST phase 0 (provisioning) exchange, where a PAC is provisioned in the supplicant. Cisco TrustSec does not perform the EAP-FAST phase 0 exchange again until the PAC expires and only performs EAP-FAST phase 1 and phase 2 exchanges for future link bringups. The EAP-FAST phase 1 exchange uses the PAC to mutually authenticate the authentication server and the supplicant. Cisco TrustSec uses the device credentials only during the PAC provisioning (or reprovisioning) steps.

The authentication server uses a temporarily configured password to authenticate the supplicant when the supplicant first joins the Cisco TrustSec network. When the supplicant first joins the Cisco TrustSec network, the authentication server authenticates the supplicant using a manufacturing certificate and then generates a strong password and pushes it to the supplicant with the PAC. The authentication server also keeps the new password in its database. The authentication server and the supplicant use this password for mutual authentication in all future EAP-FAST phase 0 exchanges.

**User Credentials**

Cisco TrustSec does not require a specific type of user credentials for endpoint devices. You can choose any type of authentication method for the user (for example, MSCHAPv2, LEAP, generic token card (GTC), or OTP) and use the corresponding credentials. Cisco TrustSec performs user authentication inside the EAP-FAST tunnel as part of the EAP-FAST phase 2 exchange.

**SGACLs and SGTs**

In security group access lists (SGACLs), you can control the operations that users can perform based on assigned security groups. The grouping of permissions into a role simplifies the management of the security policy. As you add users to a Cisco NX-OS device, you simply assign one or more security groups and they immediately receive the appropriate permissions. You can modify security groups to introduce new privileges or restrict current permissions.

Cisco TrustSec assigns a unique 16-bit tag, called the security group tag (SGT), to a security group. The number of SGTs in a Cisco NX-OS device is limited to the number of authenticated network entities. The SGT is a single label that indicates the privileges of the source within the entire enterprise. Its scope is global within a Cisco TrustSec network.

The management server derives the SGTs based on the security policy configuration. You do not have to configure them manually.

Once authenticated, Cisco TrustSec tags any packet that originates from a device with the SGT that represents the security group to which the device is assigned. The packet carries this SGT throughout the network within the Cisco TrustSec header. Because this tag represents the group of the source, the tag is referred to as the source SGT. At the egress edge of the network, Cisco TrustSec determines the group that is assigned to the packet destination device and applies the access control policy.

Cisco TrustSec defines access control policies between the security groups. By assigning devices within the network to security groups and applying access control between and within the security groups, Cisco TrustSec essentially achieves access control within the network.
Determining the Source Security Group

A network device at the ingress of the Cisco TrustSec network cloud needs to determine the SGT of the packet entering the Cisco TrustSec network cloud so that it can tag the packet with that SGT when it forwards it into the Cisco TrustSec network cloud. The egress network device needs to determine the SGT of the packet so that it can apply the SGACLs.

The network device can determine the SGT for a packet using one of the following methods:

- Obtain the source SGT during policy acquisition—After the Cisco TrustSec authentication phase, a network device acquires a policy from an authentication server. The authentication server indicates
whether the peer device is trusted or not. If a peer device is not trusted, the authentication server can also provide an SGT to apply to all packets coming from the peer device.

- Obtain the source SGT field from the Cisco TrustSec header—if a packet comes from a trusted peer device, the Cisco TrustSec header carries the correct SGT field if the network device is not the first network device in the Cisco TrustSec network cloud for the packet.

- Look up the source SGT based on the source IP address—in some cases, you can manually configure the policy to decide the SGT of a packet based on the source IP address. The SGT Exchange Protocol (SXP) can also populate the IP-address-to-SGT mapping table.

### Determining the Destination Security Group

The egress network device in a Cisco TrustSec network cloud determines the destination group for applying the SGACL. In some cases, ingress devices or other nonegress devices might have destination group information available. In those cases, SGACLs might be applied in these devices rather than in egress devices.

Cisco TrustSec determines the destination group for the packet in the following ways:

- Destination SGT of the egress port obtained during the policy acquisition
- Destination SGT lookup based on the destination IP address

Do not configure the destination SGT to enforce Cisco TrustSec on egress broadcast, multicast, and unknown unicast traffic on Fabric Extender (FEX) or vEthernet ports. Instead, set the DST to zero (unknown). The following is an example of the correct configuration:

```
cs role-based access-list acl-on-fex-egress
deny udp
deny ip
cts role-based sgt 9 dst 0 access-list acl-on-fex-egress
```

### SXP for SGT Propagation Across Legacy Access Networks

The Cisco NX-OS device hardware in the access layer supports Cisco TrustSec. Without the Cisco TrustSec hardware, the Cisco TrustSec software cannot tag the packets with SGTs. You can use SXP to propagate the SGTs across network devices that do not have hardware support for Cisco TrustSec.

SXP operates between access layer devices and distribution layer devices. The access layer devices use SXP to pass the IP addresses of the Cisco TrustSec-authenticated devices with their SGTs to the distribution switches. Distribution devices with both Cisco TrustSec-enabled software and hardware can use this information to tag packets appropriately and enforce SGACL policies.

Figure 11: Using SXP to Propagate SGT Information

This figure shows how to use SXP to propagate SGT information in a legacy network.
Tagging packets with SGTs requires hardware support. You might have devices in your network that cannot tag packets with SGTs. To allow these devices to send IP address-to-SGT mappings to a device that has Cisco TrustSec-capable hardware, you must manually set up the SXP connections. Manually setting up an SXP connection requires the following:

- If you require SXP data integrity and authentication, you must configure the same SXP password on both of the peer devices. You can configure the SXP password either explicitly for each peer connection or globally for the device. The SXP password is not required.

- You must configure each peer on the SXP connection as either an SXP speaker or an SXP listener. The speaker device distributes the SXP information to the listener device.

- You can specify a source IP address to use for each peer relationship or you can configure a default source IP address for peer connections where you have not configured a specific source IP address.

Authorization and Policy Acquisition

After authentication ends, the supplicant and AT obtain the security policy from the authentication server. The supplicant and AT enforce the policy against each other. Both the supplicant and AT provide the peer device ID that each receives after authentication. If the peer device ID is not available, Cisco TrustSec can use a manually configured peer device ID.

The authentication server returns the following policy attributes:

**Cisco TrustSec Trust**
Indicates whether the neighbor device is to be trusted for the purpose of putting the SGT in the packets.

**Peer SGT**
Indicates the security group that the peer belongs to. If the peer is not trusted, all packets received from the peer are tagged with the SGT configured on the ingress interface. If enforcement is enabled on this interface, the SGACLs that are associated with the peer SGT are downloaded. If the device does not know if the SGACLs are associated with the peer’s SGT, the device might send a follow-up request to fetch the SGACLs.

**Authorization expiry time**
Indicates the number of seconds before the policy expires. The Cisco-proprietary attribute-value (AV) pairs indicate the expiration time of an authorization or policy response to a Cisco TrustSec device. A Cisco TrustSec device should refresh its policy and authorization before it times out.
Each Cisco TrustSec device should support some minimal default access policy in case it is not able to contact the authentication server to get an appropriate policy for the peer.

Environment Data Download

The Cisco TrustSec environment data is a collection of information or policies that assists a device to function as a Cisco TrustSec node. The device acquires the environment data from the authentication server when the device first joins a Cisco TrustSec network cloud, although you might also manually configure some of the data on a device. For example, you must configure the seed Cisco TrustSec device with the authentication server information, which can later be augmented by the server list that the device acquires from the authentication server.

If you have manually configured the Cisco TrustSec device ID, but not using the AAA server for a Cisco TrustSec deployment, you should remove the Cisco TrustSec device ID by using the `no cts device-id` command. Otherwise, the following false syslog error is generated:

```
ENVIRONMENT_DATA_DOWNLOAD_FAILURE: Environment data download failed from AAA
```

The `no cts device-id` command is supported from Cisco NX-OS Release 7.2. If you are using Cisco NX-OS Release 6.2.6 or a later release, you can disable only by disabling Cisco TrustSec and reapplying Cisco TrustSec configurations without the `cts device-id` configuration.

The device must refresh the Cisco TrustSec environment data before it expires. The device can also cache the data and reuse it after a reboot if the data has not expired.

The device uses RADIUS to acquire the following environment data from the authentication server:

- **Server lists**
  - List of servers that the client can use for future RADIUS requests (for both authentication and authorization)

- **Device SGT**
  - Security group to which the device itself belongs

- **Expiry timeout**
  - Interval that controls how often the Cisco TrustSec device should refresh its environment data

RADIUS Relay Functionality

The Cisco NX-OS device that plays the role of the Cisco TrustSec AT in the 802.1X authentication process has IP connectivity to the authentication server, which allows it to acquire the policy and authorization from the authentication server by exchanging RADIUS messages over UDP/IP. The supplicant device may not have IP connectivity with the authentication server. In such cases, Cisco TrustSec allows the AT to act as a RADIUS relay for the supplicant.

The supplicant sends a special EAP over LAN (EAPOL) message to the Cisco TrustSec AT that contains the RADIUS server IP address and UDP port and the complete RADIUS request. The Cisco TrustSec AT extracts the RADIUS request from the received EAPOL message and sends it over UDP/IP to the authentication server. When the RADIUS response returns from the authentication server, the Cisco TrustSec AT forwards the message back to the supplicant, encapsulated in an EAPOL frame.
Licensing Requirements for Cisco TrustSec

The following table shows the licensing requirements for this feature:

Table 11: Licensing Requirements for Cisco TrustSec

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>Beginning with Cisco NX-OS Release 6.1, Cisco TrustSec requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For releases earlier than Cisco NX-OS 6.1, Cisco TrustSec requires an Advanced Services license. Cisco TrustSec licensing does not have a grace period. You must obtain and install an Advanced Services license before you can use Cisco TrustSec.</td>
</tr>
</tbody>
</table>

Note For an explanation of the Cisco NX-OS licensing scheme and how to obtain and apply licenses, see the Cisco NX-OS Licensing Guide.

Prerequisites for Cisco TrustSec

Cisco TrustSec has the following prerequisites:

- You must install the Advanced Services license if your device is running a release earlier than Cisco NX-OS Release 6.1.
- You must enable the 802.1X feature before you enable the Cisco TrustSec feature. Although none of the 802.1X interface level features are available, 802.1X is required for the device to authenticate with RADIUS.

Guidelines and Limitations for Cisco TrustSec

Please see the Cisco Nexus 7000 I/O Module Comparison Matrix for hardware support for Cisco TrustSec’s MACSec (802.1ae).

Cisco TrustSec has the following guidelines and limitations:

- Cisco TrustSec SGT supports IPv4 addressing only.
- Cisco TrustSec SGT in-line tagging is not supported over OTV, VXLAN, FCoE, or Programmable Fabric.
- SXP cannot use the management (mgmt 0) interface.
- You cannot enable Cisco TrustSec on interfaces in half-duplex mode.
- If SGACL is applied to the packets being routed through SVI, SGACL has to be enabled on all the VLANs and the VRF instance involved.
• You cannot configure both Cisco TrustSec and 802.1X on an interface; you can configure only one or the other. However, you must enable the 802.1X feature for Cisco TrustSec to use EAP-FAST authentication.

• AAA authentication and authorization for Cisco TrustSec is only supported by the Cisco Secure Access Control Server (ACS) and Cisco Identity Services Engine (ISE).

Default Settings for Cisco TrustSec Parameters

This table lists the default settings for Cisco TrustSec parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco TrustSec</td>
<td>Disabled</td>
</tr>
<tr>
<td>SXP</td>
<td>Disabled</td>
</tr>
<tr>
<td>SXP default password</td>
<td>None</td>
</tr>
<tr>
<td>SXP reconcile period</td>
<td>120 seconds (2 minutes)</td>
</tr>
<tr>
<td>SXP retry period</td>
<td>60 seconds (1 minute)</td>
</tr>
<tr>
<td>Caching</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Configuring Cisco TrustSec

This section provides information about the configuration tasks for Cisco TrustSec.

Enabling the Cisco TrustSec SGT Feature

You must enable both the 802.1X feature and the Cisco TrustSec feature on the Cisco NX-OS device before you can configure Cisco TrustSec.

Note

You cannot disable the 802.1X feature after you enable the Cisco TrustSec feature.

Before you begin

Ensure that you have installed the Advanced Services license, if your device is running a release earlier than Cisco NX-OS Release 6.1.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> feature dot1x</td>
<td>Enables the 802.1X feature.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# feature dot1x</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> feature cts</td>
<td>Enables the Cisco TrustSec feature.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# feature cts</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# exit</td>
<td></td>
</tr>
<tr>
<td>switch#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) show cts</td>
<td>Displays the Cisco TrustSec configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# show cts</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> (Optional) show feature</td>
<td>Displays the enabled status for features.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# show feature</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> (Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Cisco TrustSec Device Credentials

You must configure unique Cisco TrustSec credentials on each Cisco TrustSec-enabled Cisco NX-OS device in your network. Cisco TrustSec uses the password in the credentials for device authentication.

**Note**

You must also configure the Cisco TrustSec credentials for the Cisco NX-OS device on the Cisco Secure ACS. See the documentation at:

Before you begin

Ensure that you have enabled Cisco TrustSec.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>cts device-id name password password</td>
<td>Configures a unique device ID and password. The name argument has a maximum length of 32 characters and is case sensitive.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# cts device-id MyDevice1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>password CiscO321</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td>To remove the configuration of device ID and the password, use the no form of the command.</td>
</tr>
<tr>
<td>3</td>
<td>exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch#</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>(Optional) show cts</td>
<td>Displays the Cisco TrustSec configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# show cts</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>(Optional) show cts environment</td>
<td>Displays the Cisco TrustSec environment data.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# show cts environment</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

Enabling the Cisco TrustSec SGT Feature, on page 113

Configuring AAA for Cisco TrustSec

You can use Cisco Secure ACS for Cisco TrustSec authentication. You must configure RADIUS server groups and specify the default AAA authentication and authorization methods on one of the Cisco TrustSec-enabled Cisco NX-OS devices in your network cloud. Because Cisco TrustSec supports RADIUS relay, you need to configure AAA only on a seed Cisco NX-OS device that is directly connected to a Cisco Secure ACS. For all the other Cisco TrustSec-enabled Cisco NX-OS devices, Cisco TrustSec automatically provides a private
AAA server group, aaa-private-sg. The seed Cisco NX-OS devices uses the management virtual routing and forwarding (VRF) instance to communicate with the Cisco Secure ACS.

**Note**
Only the Cisco Secure ACS supports Cisco TrustSec.

### Configuring AAA on a Seed Cisco NX-OS Device in a Cisco TrustSec Network

This section describes how to configure AAA on the seed Cisco NX-OS device in your Cisco TrustSec network cloud.

**Note**
When you configure the AAA RADIUS server group for the seed Cisco NX-OS device, you must specify a VRF instance. If you use the management VRF instance, no further configuration is necessary for the nonseed devices in the network cloud. If you use a different VRF instance, you must configure the nonseed devices with that VRF instance.

**Before you begin**
- Obtain the IPv4 or IPv6 address or hostname for the Cisco Secure ACS.
- Ensure that you enabled Cisco TrustSec.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>radius-server host {ipv4-address</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# radius-server host 10.10.1.1 key L1a0K2s9 pac</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) show radius-server</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# show radius-server</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>aaa group server radius group-name</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><code>switch(config)# aaa group server radius Rad1</code>&lt;br&gt;<code>switch(config-radius)#</code></td>
<td>Specifies the RADIUS server host address.</td>
</tr>
</tbody>
</table>

**Step 5**

**server** `{ipv4-address | ipv6-address | hostname}`

**Example:**
`switch(config-radius)# server 10.10.1.1`

Specifies the management VRF instance for the AAA server group.

**Note**  
If you use the management VRF instance, no further configuration is necessary for the nonseed devices in the network cloud. If you use a different VRF instance, you must configure the nonseed devices with that VRF instance.

**Step 6**

**use-vrf vrf-name**

**Example:**
`switch(config-radius)# use-vrf management`

**Step 7**

**exit**

**Example:**
`switch(config-radius)# exit<br>switch(config)#`

Exits RADIUS server group configuration mode.

**Step 8**

**aaa authentication dot1x default group group-name**

**Example:**
`switch(config)# aaa authentication dot1x default group Rad1`

Specifies the RADIUS server groups to use for 802.1X authentication.

**Step 9**

**aaa authorization cts default group group-name**

**Example:**
`switch(config)# aaa authentication cts default group Rad1`

Specifies the RADIUS server groups to use for Cisco TrustSec authorization.

**Step 10**

**exit**

**Example:**
`switch(config)# exit<br>switch#`

Exits global configuration mode.

**Step 11**

(Optional) **show radius-server groups [group-name]**

**Example:**
`switch# show radius-server group rad1`

Displays the RADIUS server group configuration.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 12**<br>
(Optional) show aaa authentication<br>
Example: <br>switch# show aaa authentication | Displays the AAA authentication configuration. |
| **Step 13**<br>
(Optional) show aaa authorization<br>
Example: <br>switch# show aaa authorization | Displays the AAA authorization configuration. |
| **Step 14**<br>
(Optional) show cts pacs<br>
Example: <br>switch# show cts pacs | Displays the Cisco TrustSec PAC information. |
| **Step 15**<br>
(Optional) copy running-config startup-config<br>
Example: <br>switch# copy running-config startup-config | Copies the running configuration to the startup configuration. |

**Related Topics**
- [Enabling the Cisco TrustSec SGT Feature](#), on page 113
- [Configuring AAA on Cisco TrustSec Nonseed Cisco NX-OS Devices](#), on page 118

## Configuring AAA on Cisco TrustSec Nonseed Cisco NX-OS Devices

Cisco TrustSec configures an AAA server group named aaa-private-sg on the nonseed Cisco NX-OS devices in the network cloud. By default, the aaa-private-sg server group uses the management VRF instance to communicate with the Cisco Secure ACS and no further configuration is required on the nonseed Cisco NX-OS devices. However, if you choose to use a different VRF instance, you must change the aaa-private-sg on the nonseed Cisco NX-OS device to use the correct VRF instance.

**Before you begin**

Ensure that you enabled Cisco TrustSec.

Ensure that you have configured a seed Cisco NX-OS device in your network.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**<br>configure terminal<br>
Example: <br>switch# configure terminal<br>switch(config)# | Enters global configuration mode. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>aaa group server radius aaa-private-sg</td>
<td>Specifies the RADIUS server group aaa-private-sg and enters RADIUS server group configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# aaa group server radius aaa-private-sg</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-radius)#</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>use-vrf vrf-name</td>
<td>Specifies the management VRF instance for the AAA server group.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-radius)# use-vrf MyVRF</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>Exits RADIUS server group configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-radius)# exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>(Optional) show radius-server groups aaa-private-sg</td>
<td>Displays the RADIUS server group configuration for the default server group.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# show radius-server groups aaa-private-sg</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**
- Enabling the Cisco TrustSec SGT Feature, on page 113
- Configuring AAA on a Seed Cisco NX-OS Device in a Cisco TrustSec Network, on page 116

**Configuring Cisco TrustSec Authentication, Authorization, and Data Path Security**

This section provides information about the configuration tasks for Cisco TrustSec authentication, authorization, and data path security.

**Cisco TrustSec Configuration Process for Cisco TrustSec Authentication and Authorization**

Follow these steps to configure Cisco TrustSec authentication and authorization:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enable the Cisco TrustSec feature. See Enabling the Cisco TrustSec SGT Feature, on page 113.</td>
</tr>
<tr>
<td>2</td>
<td>Enable Cisco TrustSec authentication. See Enabling Cisco TrustSec Authentication, on page 120.</td>
</tr>
</tbody>
</table>
Step 3  Enable 802.1X authentication for Cisco TrustSec on the interfaces. See Enabling the 802.1X Feature, on page 82.

Related Topics
- Enabling the Cisco TrustSec SGT Feature, on page 113
- Enabling Cisco TrustSec Authentication, on page 120

Enabling Cisco TrustSec Authentication

You must enable Cisco TrustSec authentication on the interfaces.

Caution
For the Cisco TrustSec authentication configuration to take effect, you must enable and disable the interface, which disrupts traffic on the interface.

Note
Enabling 802.1X mode for Cisco TrustSec automatically enables authorization.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  configure terminal
  **Example:**
  switch# configure terminal
  switch(config)# | Enters global configuration mode. |
| **Step 2**
  interface ethernet *slotport [ - port2]*
  **Example:**
  switch(config)# interface ethernet 2/2
  switch(config-if)# | Specifies a single port or a range of ports and enters interface configuration mode. |
| **Step 3**
  cts dot1x
  **Example:**
  switch(config-if)# cts dot1x
  switch(config-if-cts-dot1x)# | Enables 802.1X authentication for Cisco TrustSec and enters Cisco TrustSec 802.1X configuration mode. |
| **Step 4**
  (Optional) no replay-protection
  **Example:**
  switch(config-if-cts-dot1x)# no replay-protection | Disables replay protection. The default is enabled. |
| **Step 5**
  exit
  **Example:**
  switch(config-if-cts-dot1x)# exit
  switch(config-if)# | Exits Cisco TrustSec 802.1X configuration mode. |
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>shutdown</td>
<td>Disables the interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)# shutdown</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>no shutdown</td>
<td>Enables the interface and enables Cisco TrustSec authentication on the interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)# no shutdown</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>(Optional) show cts interface {all</td>
<td>ethernet slot/port}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# show cts interface all</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

- Enabling the Cisco TrustSec SGT Feature, on page 113

### Configuring Data-Path Replay Protection for Cisco TrustSec on Interfaces

By default, the Cisco NX-OS software enables the data-path reply protection feature. You can disable the data-path reply protection feature on the interfaces for Layer 2 Cisco TrustSec if the connecting device does not support SA protocol.

⚠️ **Caution**

For the data-path replay protection configuration to take effect, you must enable and disable the interface, which disrupts traffic on the interface.

### Before you begin

Ensure that you enabled Cisco TrustSec authentication on the interface.
## Configuring Data-Path Replay Protection for Cisco TrustSec on Interfaces

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | configure terminal | Enters global configuration mode.  
**Example:**  
switch# configure terminal  
switch(config)# |
| **Step 2** | interface ethernet slotport [-port2] | Specifies a single port or a range of ports and enters interface configuration mode.  
**Example:**  
switch(config)# interface ethernet 2/2  
switch(config-if)# |
| **Step 3** | cts dot1x | Enables 802.1X authentication for Cisco TrustSec and enters Cisco TrustSec 802.1X configuration mode.  
**Example:**  
switch(config-if)# cts dot1x  
switch(config-if-cts-dot1x)# |
| **Step 4** | no replay-protection | Disables data-path replay protection. The default is enabled.  
**Example:**  
switch(config-if-cts-dot1x)# no replay-protection |
| **Step 5** | exit | Exits Cisco TrustSec 802.1X configuration mode.  
**Example:**  
switch(config-if-cts-dot1x)# exit  
switch(config-if)# |
| **Step 6** | shutdown | Disables the interface.  
**Example:**  
switch(config-if)# shutdown |
| **Step 7** | no shutdown | Enables the interface and disables the data-path reply protection feature on the interface.  
**Example:**  
switch(config-if)# no shutdown |
| **Step 8** | exit | Exits interface configuration mode.  
**Example:**  
switch(config-if)# exit  
switch(config)# |
| **Step 9** | (Optional) show cts interface {all | ethernet slotport} | Displays the Cisco TrustSec configuration on the interface.  
**Example:**  
switch(config)# show cts interface all |
Related Topics

Enabling Cisco TrustSec Authentication, on page 120

Configuring SGT Propagation for Cisco TrustSec on Interfaces

The SGT propagation feature on the Layer 2 interface is enabled by default. You can disable the SGT propagation feature on an interface if the peer device connected to the interface cannot handle Cisco TrustSec packets tagged with an SGT.

⚠️ Caution

For the SGT propagation configuration to take effect, you must enable and disable the interface, which disrupts traffic on the interface.

Before you begin

Ensure that you enabled Cisco TrustSec authentication on the interface.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface ethernet slotport [ - port2]</td>
<td>Specifies a single port or a range of ports and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# interface ethernet 2/2</td>
<td></td>
</tr>
<tr>
<td>switch(config-if)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> cts dot1x</td>
<td>Enables 802.1X authentication for Cisco TrustSec and enters Cisco TrustSec 802.1X configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-if)# cts dot1x</td>
<td></td>
</tr>
<tr>
<td>switch(config-if-cts-dot1x)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no propagate-sgt</td>
<td>Disables SGT propagation. The default is enabled.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-if-cts-dot1x)# no propagate-sgt</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 5</strong> exit</td>
<td>Exits Cisco TrustSec 802.1X configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-if-cts-dot1x)# exit</td>
</tr>
<tr>
<td></td>
<td>switch(config-if)#</td>
</tr>
<tr>
<td><strong>Step 6</strong> shutdown</td>
<td>Disables the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-if)# shutdown</td>
</tr>
<tr>
<td><strong>Step 7</strong> no shutdown</td>
<td>Enables the interface and disables the data-path reply protection feature on the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-if)# no shutdown</td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-if)# exit</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td><strong>Step 9</strong> (Optional)</td>
<td>Displays the Cisco TrustSec configuration on the interface.</td>
</tr>
<tr>
<td><strong>show cts interface</strong></td>
<td>{all</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# show cts interface all</td>
</tr>
<tr>
<td><strong>Step 10</strong> (Optional)</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>copy running-config</strong></td>
<td>startup-config</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

### Related Topics

Enabling Cisco TrustSec Authentication, on page 120

### Configuring Cisco TrustSec Authentication in Manual Mode

You can manually configure Cisco TrustSec on an interface if your Cisco NX-OS device does not have access to a Cisco Secure ACS or authentication is not needed because you have the MAC address authentication bypass feature enabled. You must manually configure the interfaces on both ends of the connection.

#### Note

You cannot enable Cisco TrustSec on interfaces in half-duplex mode. Use the `show interface` command to determine if an interface is configured for half-duplex mode.
For the Cisco TrustSec manual mode configuration to take effect, you must enable and disable the interface, which disrupts traffic on the interface.

**Before you begin**

Ensure that you enabled Cisco TrustSec.

**Procedure**

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

| **Step 2**        | Specifies an interface and enters interface configuration mode. |
| interface interface slot/port| |
| Example:          |         |
| switch(config)# interface ethernet 2/2 |
| switch(config-if)# |         |

| **Step 3**        | Enters Cisco TrustSec manual configuration mode. |
| cts manual        |         |
| Example:          |         |
| switch(config-if)# cts manual |
| switch(config-if-cts-manual)# |         |

**Note**

You cannot enable Cisco TrustSec on interfaces in half-duplex mode.

| **Step 4**        | Configures a dynamic authorization policy download. The peer-name argument is the Cisco TrustSec device ID for the peer device. The peer name is case sensitive. |
| policy dynamic identity peer-name | |
| Example:          |         |
| switch(config-if-cts-manual)# policy dynamic identity MyDevice2 | |

**Note**

Ensure that you have configured the Cisco TrustSec credentials and AAA for Cisco TrustSec.

**Note**

The **policy dynamic** and **policy static** commands are mutually exclusive. Only one can be applied at a time. To change from one to the other, you must use the no form of the command to remove the configuration before configuring the other command.

<p>| <strong>Step 5</strong>        | Configures a static authorization policy. The tag argument is a hexadecimal value in the format 0xhhhh. The range is from 0x2 to 0xfffe. The trusted keyword indicates that |
| policy static sgt tag [trusted] |         |
| Example:          |         |
| switch(config-if-cts-manual)# policy static sgt 0x2 | |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>traffic coming on the interface with this SGT should not have its tag overridden. <strong>Note</strong> The <code>policy dynamic</code> and <code>policy static</code> commands are mutually exclusive. Only one can be applied at a time. To change from one to the other, you must use the <code>no</code> form of the command to remove the configuration before configuring the other command.</td>
</tr>
</tbody>
</table>

**Step 6**

**exit**

**Example:**

```
switch(config-if-cts-manual)# exit
switch(config-if)#
```

Disables the interface.

**Step 7**

**shutdown**

**Example:**

```
switch(config-if)# shutdown
```

Enables the interface and enables Cisco TrustSec authentication on the interface.

**Step 8**

**no shutdown**

**Example:**

```
switch(config-if)# no shutdown
```

Exits Cisco TrustSec manual configuration mode.

**Step 9**

**exit**

**Example:**

```
switch(config-if)# exit
switch(config)#
```

Displays the Cisco TrustSec configuration for the interfaces.

**Step 10**

**(Optional)** `show cts interface {all | ethernet slot/port}`

**Example:**

```
switch# show cts interface all
```

Copies the running configuration to the startup configuration.

**Step 11**

**(Optional)** `copy running-config startup-config`

**Example:**

```
switch# copy running-config startup-config
```

Related Topics

[Enabling the Cisco TrustSec SGT Feature](#), on page 113

**Configuring SGACL Policies**

This section provides information about the configuration tasks for SGACL policies.
SGACL Policy Configuration Process

Follow these steps to configure Cisco TrustSec SGACL policies:

**Procedure**

**Step 1**
To improve performance, globally enable SGACL batch programming.

**Step 2**
For Layer 2 interfaces, enable SGACL policy enforcement for the VLANs with Cisco TrustSec-enabled interfaces.

**Step 3**
For Layer 3 interfaces, enable SGACL policy enforcement for the VRF instances with Cisco TrustSec-enabled interfaces.

**Step 4**
If you are not using AAA on a Cisco Secure ACS to download the SGACL policy configuration, manually configure the SGACL mapping and policies.

Enabling SGACL Policy Enforcement on VLANs

If you use SGACLs, you must enable SGACL policy enforcement in the VLANs that have Cisco TrustSec-enabled Layer 2 interfaces.

**Note**

This operation cannot be performed on FCoE VLANs.

**Before you begin**

- Ensure that you enabled Cisco TrustSec.
- Ensure that you enabled SGACL batch programming.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  configure terminal
  
  **Example:**
  switch# configure terminal
  switch(config)# | Enters global configuration mode. |
| **Step 2**
  vlan vlan-id
  
  **Example:**
  switch(config)# vlan 10
  switch(config-vlan)# | Specifies a VLAN and enters VLAN configuration mode. |
| **Step 3**
  cts role-based enforcement
  
  **Example:** | Enables Cisco TrustSec SGACL policy enforcement on the VLAN. |
### Enabling SGACL Policy Enforcement on VRF Instances

If you use SGACLs, you must enable SGACL policy enforcement in the VRF instances that have Cisco TrustSec-enabled Layer 3 interfaces.

#### Related Topics

- [Enabling the Cisco TrustSec SGT Feature](#), on page 113

#### Note

You cannot enable SGACL policy enforcement on the management VRF instance.

### Before you begin

- Ensure that you enabled Cisco TrustSec.
- Ensure that you enabled SGACL batch programming.
- Ensure that you enabled dynamic Address Resolution Protocol (ARP) inspection or Dynamic Host Configuration Protocol (DHCP) snooping.

---

### Command or Action | Purpose
---|---
switch(config-vlan)# cts role-based enforcement | **Note** If you enable the cts role-based enforcement on a VLAN and no other configuration on ports, the traffic traversing through these ports are subject to (0,0) SGACL. You can either configure this SGACL statically or download it from Cisco ISE.

**Step 4**

**exit**

**Example:**

```
switch(config-vlan)# exit
switch(config)#
```

Saves the VLAN configuration and exits VLAN configuration mode.

**Step 5**

(Optional) **show cts role-based enable**

**Example:**

```
switch(config)# show cts role-based enable
```

Displays the Cisco TrustSec SGACL enforcement configuration.

**Step 6**

(Optional) **copy running-config startup-config**

**Example:**

```
switch(config)# copy running-config startup-config
```

Copies the running configuration to the startup configuration.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies a VRF instance and enters VRF configuration mode.</td>
</tr>
<tr>
<td>vrf context vrf-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# vrf context MyVrf</td>
<td></td>
</tr>
<tr>
<td>switch(config-vrf)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables Cisco TrustSec SGACL policy enforcement on the VRF instance.</td>
</tr>
<tr>
<td>cts role-based enforcement</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-vrf)# cts role-based enforcement</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Exits VRF configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-vrf)# exit</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Displays the Cisco TrustSec SGACL enforcement configuration.</td>
</tr>
<tr>
<td>(Optional) show cts role-based enable</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# show cts role-based enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>(Optional) copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

- [Enabling the Cisco TrustSec SGT Feature](#), on page 113

### Manually Configuring Cisco TrustSec SGTs

You can manually configure unique Cisco TrustSec security group tags (SGTs) for the packets originating from this device.

**Note**

You must also configure the Cisco TrustSec credentials for the Cisco NX-OS device on the Cisco Secure ACS.

**Before you begin**

Ensure that you have enabled Cisco TrustSec.
Manually Configuring IPv4-Address-to-SGACL SGT Mapping for a VLAN

You can manually configure an IPv4 address to SGACL SGT mapping on a VLAN if you do not have Cisco Secure ACS, dynamic ARP inspection, or DHCP snooping available on your Cisco NX-OS device.

Before you begin

- Ensure that you enabled Cisco TrustSec.
- Ensure that you enabled SGACL policy enforcement on the VLAN.

Procedure

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

| **Step 2** cts sgt **tag** | Configures the SGT for packets sent from the device. The **tag** argument is a hexadecimal value in the format **0xhhhh**. The range is from 0x2 to 0xffef. |
| **Example:** | |
| switch(config)# cts sgt 0x00a2 |

| **Step 3** exit | Exits global configuration mode. |
| **Example:** | |
| switch(config)# exit |
| switch# |

| **Step 4** (Optional) **show cts environment-data** | Displays the Cisco TrustSec environment data information. |
| **Example:** | |
| switch# show cts environment-data |

| **Step 5** (Optional) **copy running-config startup-config** | Copies the running configuration to the startup configuration. |
| **Example:** | |
| switch# copy running-config startup-config |
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td><code>vlan vlan-id</code></td>
<td>Specifies a VLAN and enters VLAN configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# vlan 10</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-vlan)#</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>cts role-based sgt-map ipv4-address tag</code></td>
<td>Configures SGT mapping for the SGACL policies for the VLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-vlan)# cts role-based sgt-map 10.10.1.1 100</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>exit</code></td>
<td>Saves the VLAN configuration and exits VLAN configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-vlan)# exit</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><em>(Optional) show cts role-based sgt-map</em></td>
<td>Displays the Cisco TrustSec SGACL SGT mapping configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# show cts role-based sgt-map</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><em>(Optional) copy running-config startup-config</em></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics
- Enabling the Cisco TrustSec SGT Feature, on page 113
- Enabling SGACL Policy Enforcement on VLANs, on page 127
- Enabling SGACL Policy Enforcement on VRF Instances, on page 128

### Manually Configuring IPv4-Address-to-SGACL SGT Mapping for a VRF Instance

You can manually configure IPv4-address-to-SGACL SGT mapping on a VRF instance if a Cisco Secure ACS is not available to download the SGACL policy configuration. You can use this feature if you do not have Cisco Secure ACS, dynamic ARP inspection, or DHCP snooping available on your Cisco NX-OS device.

### Before you begin
- Ensure that you enabled Cisco TrustSec.
- Ensure that you enabled SGACL policy enforcement on the VRF instance.
- Ensure that the Layer-3 module is enabled.
Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> vrf context vrf-name</td>
<td>Specifies a VRF instance and enters VRF configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# vrf context accounting</td>
<td></td>
</tr>
<tr>
<td>switch(config-vrf)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> cts role-based sgt-map ipv4-address tag</td>
<td>Configures SGT mapping for the SGACL policies for the VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-vrf)# cts role-based sgt-map 10.10.1.1 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits VRF configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-vrf)# exit</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) show cts role-based sgt-map</td>
<td>Displays the Cisco TrustSec SGACL SGT mapping configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# show cts role-based sgt-map</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> (Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Manually Configuring SGACL Policies

You can manually configure SGACL policies on your Cisco NX-OS device if a Cisco Secure ACS is not available to download the SGACL policy configuration.

**Before you begin**

Ensure that you have enabled Cisco TrustSec.

For Cisco TrustSec logging to function, you must enable Cisco TrustSec counters or statistics.

Ensure that you have enabled SGACL policy enforcement on the VLAN and VRF instance.
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> cts role-based access-list list-name</td>
<td>Specifies an SGACL and enters role-based access list configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# cts role-based access-list MySGACL</td>
<td></td>
</tr>
<tr>
<td>switch(config-rbacl)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) {deny</td>
<td>permit} all</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-rbacl)# deny all</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) {deny</td>
<td>permit} icmp</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-rbacl)# permit icmp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) {deny</td>
<td>permit} igmp</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-rbacl)# deny igmp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> (Optional) {deny</td>
<td>permit} ip</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-rbacl)# permit ip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> (Optional) {deny</td>
<td>permit} tcp [{dst</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-rbacl)# deny tcp dst eq 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> {deny</td>
<td>permit} udp [{dst</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-rbacl)# permit udp src eq 1312</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> exit</td>
<td>Exits role-based access-list configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config-rbacl)# exit</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Maps the SGT values to the SGACL. The <code>sgt-value</code> and <code>dgt-value</code> argument values range from 0 to 65520.</td>
</tr>
<tr>
<td>`cts role-based sgt {sgt-value</td>
<td>any</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You must create the SGACL before you can map SGTs to it.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Displays the Cisco TrustSec SGACL configuration.</td>
</tr>
<tr>
<td><code>(Optional) show cts role-based access-list</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# show cts role-based access-list</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><code>(Optional) copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

**Related Topics**
- Enabling the Cisco TrustSec SGT Feature, on page 113
- Enabling SGACL Policy Enforcement on VLANs, on page 127
- Enabling SGACL Policy Enforcement on VRF Instances, on page 128

## Displaying the Downloaded SGACL Policies

After you configure the Cisco TrustSec device credentials and AAA, you can verify the Cisco TrustSec SGACL policies downloaded from the Cisco Secure ACS. The Cisco NX-OS software downloads the SGACL policies when it learns of a new SGT through authentication and authorization on an interface, from SXP, or from manual IPv4 address to SGACL SGT mapping.

### Before you begin

Ensure that you enabled Cisco TrustSec.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Displays Cisco TrustSec SGACLs, both downloaded from the Cisco Secure ACS and manually configured on the Cisco NX-OS device.</td>
</tr>
<tr>
<td><code>show cts role-based access-list</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# show cts role-based access-list</td>
</tr>
</tbody>
</table>

**Related Topics**
- Enabling the Cisco TrustSec SGT Feature, on page 113
Refreshing the Downloaded SGACL Policies

You can refresh the SGACL policies downloaded to the Cisco NX-OS device by the Cisco Secure ACS.

**Before you begin**

Ensure that you enabled Cisco TrustSec.

**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>cts refresh role-based-policy</code></td>
<td>Refreshes the Cisco TrustSec SGACL policies from the Cisco Secure ACS.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch# cts refresh role-based-policy</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional) <code>show cts role-based policy</code></td>
<td>Displays the Cisco TrustSec SGACL policies.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch# show cts role-based policy</code></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

[Enabling the Cisco TrustSec SGT Feature](#), on page 113

Clearing Cisco TrustSec SGACL Policies

You can clear the Cisco TrustSec SGACL policies.

**Before you begin**

Ensure that you enabled Cisco TrustSec.

**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>(Optional) <code>show cts role-based policy</code></td>
<td>Displays the Cisco TrustSec RBACL policy configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch# clear cts policy all</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>`clear cts policy {all</td>
<td>peer device-name</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch# clear cts policy all</code></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

[Enabling the Cisco TrustSec SGT Feature](#), on page 113
Manually Configuring SXP

You can use the SGT Exchange Protocol (SXP) to propagate the SGTs across network devices that do not have hardware support for Cisco TrustSec. This section describes how to configure Cisco TrustSec SXP on Cisco NX-OS devices in your network.

Cisco TrustSec SXP Configuration Process

Follow these steps to manually configure Cisco TrustSec SXP:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>cts sxp enable</td>
<td>Enables SXP for Cisco TrustSec.</td>
</tr>
</tbody>
</table>

Before you begin

Ensure that you enabled Cisco TrustSec.

Related Topics

- Enabling SGACL Policy Enforcement on VLANs, on page 127
- Manually Configuring IPv4-Address-to-SGACL SGT Mapping for a VLAN, on page 130
- Manually Configuring SGACL Policies, on page 132
- Enabling SGACL Policy Enforcement on VRF Instances, on page 128
- Enabling the Cisco TrustSec SGT Feature, on page 113
- Enabling Cisco TrustSec SXP, on page 136
- Configuring Cisco TrustSec SXP Peer Connections, on page 137
### Related Topics

- [Enabling the Cisco TrustSec SGT Feature](#), on page 113

---

### Configuring Cisco TrustSec SXP Peer Connections

You must configure the SXP peer connection on both the speaker and listener devices. When using password protection, make sure to use the same password on both ends.

**Note**

If the default SXP source IP address is not configured and you do not specify the SXP source address in the connection, the Cisco NX-OS software derives the SXP source IP address from existing local IP addresses. The SXP source address could be different for each TCP connection initiated from the Cisco NX-OS device.

**Before you begin**

- Ensure that you enabled Cisco TrustSec.
- Ensure that you enabled SXP.
- Ensure that you enabled RBACL policy enforcement in the VRF instance.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**

```
switch(config)# configure terminal
```

Example:

```
switch# configure terminal
switch(config)#
```

Enters global configuration mode.

| **Step 2**

```
switch(config)# cts sxp connection peer peer-ipv4-addr
```

Example:

```
switch(config)# cts sxp connection peer peer-ipv4-addr
```

Configures the SXP address connection.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `none | required password` mode {speaker listener} [vrf vrf-name] | The `source` keyword specifies the IPv4 address of the source device. The default source is IPv4 address you configured using the `cts sxp default source-ip` command. The `password` keyword specifies the password that SXP should use for the connection using the following options:  
  - Use the `default` option to use the default SXP password that you configured using the `cts sxp default password` command.  
  - Use the `none` option to not use a password.  
  - Use the `required` option to use the password specified in the command.  
  The `speaker` and `listener` keywords specify the role of the remote peer device.  
  The `vrf` keyword specifies the VRF instance to the peer. The default is the default VRF instance.  
  **Note** You cannot use the management (mgmt 0) interface for SXP. |

**Step 3**  
**Example:**  
```bash  
switch(config)# cts sxp connection peer 10.10.1.1 source 20.20.1.1 password default mode listener  
```

Exits global configuration mode.  
**Step 4**  
**Example:**  
```bash  
switch(config)# exit  
switch#  
```

Displays the SXP connections and their status.  
**Step 5**  
**Example:**  
```bash  
switch# show cts sxp connections  
```

Copies the running configuration to the startup configuration.  
Related Topics  
- Enabling the Cisco TrustSec SGT Feature, on page 113  
- Enabling Cisco TrustSec SXP, on page 136  
- Enabling SGACL Policy Enforcement on VRF Instances, on page 128
Configuring the Default SXP Password

By default, SXP uses no password when setting up connections. You can configure a default SXP password for the Cisco NX-OS device.

Before you begin

Ensure that you enabled Cisco TrustSec.

Ensure that you enabled SXP.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:**
  switch# configure terminal
  switch(config)# | |
| **Step 2** cts sxp default password *password* | Configures the SXP default password. |
| **Example:**
  switch(config)# cts sxp default password A2Q3d4F5 | |
| **Step 3** exit | Exits global configuration mode. |
| **Example:**
  switch(config)# exit
  switch# | |
| **Step 4** (Optional) show cts sxp | Displays the SXP configuration. |
| **Example:**
  switch# show cts sxp | |
| **Step 5** (Optional) show running-config cts | Displays the SXP configuration in the running configuration. |
| **Example:**
  switch# show running-config cts | |
| **Step 6** (Optional) copy running-config startup-config | Copies the running configuration to the startup configuration. |
| **Example:**
  switch# copy running-config startup-config | |

Related Topics

  - Enabling the Cisco TrustSec SGT Feature, on page 113
  - Enabling Cisco TrustSec SXP, on page 136
Configuring the Default SXP Source IPv4 Address

The Cisco NX-OS software uses the default source IPv4 address in all new TCP connections where a source IPv4 address is not specified. When you change the default source IP address, the existing SXP connections are reset and the IP-SGT bindings learned over SXP are cleared. The SXP connections, for which a source IP address has been configured, will continue to use the same IP address, while coming back up.

The SXP connections, for which a source IP address has not been configured, uses the default IP address as the source IP address. Note that for such connections, correct destination IP address configuration on the peer and the reachability to the default source IP address are the required conditions before such connections can become operational. It is recommended to ensure that these conditions are met for existing operational connections, before configuring default source IP address on a device.

Before you begin

Ensure that you enabled Cisco TrustSec.

Ensure that you enabled SXP.

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>switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>cts sxp default source-ip src-ip-addr</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# cts sxp default source-ip 10.10.3.3</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# exit</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) <strong>show cts sxp</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>switch# show cts sxp</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) <strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>

Related Topics

- Enabling the Cisco TrustSec SGT Feature, on page 113
- Enabling Cisco TrustSec SXP, on page 136
Changing the SXP Reconcile Period

After a peer terminates an SXP connection, an internal hold-down timer starts. If the peer reconnects before the internal hold-down timer expires, the SXP reconcile period timer starts. While the SXP reconcile period timer is active, the Cisco NX-OS software retains the SGT mapping entries learned from the previous connection and removes invalid entries. The default value is 120 seconds (2 minutes). Setting the SXP reconcile period to 0 seconds disables the timer and causes all entries from the previous connection to be removed.

Before you begin
Ensure that you enabled Cisco TrustSec.
Ensure that you enabled SXP.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Changes the SXP reconcile timer period. The default value is 120 seconds (2 minutes). The range is from 0 to 64000.</td>
</tr>
<tr>
<td><code>cts sxp reconcile-period seconds</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# cts sxp reconcile-period 180</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# exit</td>
<td></td>
</tr>
<tr>
<td>switch#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Displays the SXP configuration.</td>
</tr>
<tr>
<td>(Optional) <code>show cts sxp</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# show cts sxp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>(Optional) <code>copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- Enabling the Cisco TrustSec SGT Feature, on page 113
- Enabling Cisco TrustSec SXP, on page 136

Changing the SXP Retry Period

The SXP retry period determines how often the Cisco NX-OS software retries an SXP connection. When an SXP connection is not successfully set up, the Cisco NX-OS software makes a new attempt to set up the
connection after the SXP retry period timer expires. The default value is 60 seconds (1 minute). Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

Before you begin
Ensure that you enabled Cisco TrustSec.
Ensure that you enabled SXP.

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>switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | |
| cts sxp retry-period *seconds* | Changes the SXP retry timer period. The default value is 60 seconds (1 minute). The range is from 0 to 64000. |
| **Example:** | |
| switch(config)# cts sxp retry-period 120 | |

| **Step 3** | |
| exit | Exits global configuration mode. |
| **Example:** | |
| switch(config)# exit | |
| switch# | |

| **Step 4** | |
| (Optional) show cts sxp | Displays the SXP configuration. |
| **Example:** | |
| switch# show cts sxp | |

| **Step 5** | |
| (Optional) copy running-config startup-config | Copies the running configuration to the startup configuration. |
| **Example:** | |
| switch# copy running-config startup-config | |

Related Topics
- Enabling the Cisco TrustSec SGT Feature, on page 113
- Enabling Cisco TrustSec SXP, on page 136

Verifying the Cisco TrustSec Configuration

To display Cisco TrustSec configuration information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show cts</td>
<td>Displays Cisco TrustSec information.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show cts credentials</td>
<td>Displays Cisco TrustSec credentials for EAP-FAST.</td>
</tr>
<tr>
<td>show cts environment-data</td>
<td>Displays Cisco TrustSec environmental data.</td>
</tr>
<tr>
<td>show cts interface {all</td>
<td>ethernet slot/port}</td>
</tr>
<tr>
<td>show cts role-based access-list</td>
<td>Displays Cisco TrustSec SGACL information.</td>
</tr>
<tr>
<td>show cts pacs</td>
<td>Displays Cisco TrustSec authorization information and PACs in the device key store.</td>
</tr>
<tr>
<td>show cts role-based enable</td>
<td>Displays Cisco TrustSec SGACL enforcement status.</td>
</tr>
<tr>
<td>show cts role-based policy</td>
<td>Displays Cisco TrustSec SGACL policy information.</td>
</tr>
<tr>
<td>show cts role-based sgt-map</td>
<td>Displays the Cisco TrustSec SGACL SGT map configuration.</td>
</tr>
<tr>
<td>show cts sxp</td>
<td>Displays Cisco TrustSec SXP information.</td>
</tr>
<tr>
<td>show running-config cts</td>
<td>Displays the Cisco TrustSec information in the running configuration.</td>
</tr>
</tbody>
</table>

## Configuration Examples for Cisco TrustSec

This section provides configuration examples for Cisco TrustSec.

### Example: Enabling Cisco TrustSec

The following example shows how to enable Cisco TrustSec:

```plaintext
feature dot1x
feature cts
cts device-id device1 password Cisco321
```

### Example: Configuring AAA for Cisco TrustSec on a Seed Cisco NX-OS Device

The following example shows how to configure AAA for Cisco TrustSec on the seed Cisco NX-OS device:

```plaintext
radius-server host 10.10.1.1 key Cisco123 pac
aaa group server radius Rad1
   server 10.10.1.1
   use-vrf management
aaa authentication dot1x default group Rad1
aaa authorization cts default group Rad1
```
Example: Enabling Cisco TrustSec Authentication on an Interface

The following example shows how to enable Cisco TrustSec authentication with a clear text password on an interface:

```
interface ethernet 2/1
  cts dot1x
  shutdown
  no shutdown
```

Example: Configuring Cisco TrustSec Authentication in Manual Mode

The following example shows how to configure Cisco TrustSec authentication in manual mode static policy on an interface:

```
interface ethernet 2/1
  cts manual
  policy static sgt 0x20
```

The following example shows how to configure Cisco TrustSec authentication in manual mode dynamic policy on an interface:

```
interface ethernet 2/2
  cts manual
  policy dynamic identity device2
```

Example: Configuring Cisco TrustSec Role-Based Policy Enforcement for the Default VRF Instance

The following example shows how to enable Cisco TrustSec role-based policy enforcement for the default VRF instance:

```
calls role-based enforcement
```

Example: Configuring Cisco TrustSec Role-Based Policy Enforcement for a Nondefault VRF

The following example shows how to enable Cisco TrustSec role-based policy enforcement for a nondefault VRF:

```
vrf context test
  calls role-based enforcement
```
Example: Configuring Cisco TrustSec Role-Based Policy Enforcement for a VLAN

The following example shows how to enable Cisco TrustSec role-based policy enforcement for a VLAN:

```
vlan 10
cis role-based enforcement
```
Example: Manually Configuring SXP Peer Connections

This figure shows an example of SXP peer connections over the default VRF instance.

Figure 12: Example SXP Peer Connections

The following example shows how to configure the SXP peer connections on SwitchA:

```plaintext
feature cts
ccts role-based enforcement
ccts sxp enable
ccts sxp connection peer 10.20.2.2 password required A2BsxpPW mode listener
ccts sxp connection peer 10.30.3.3 password required A2CsxpPW mode listener
```

The following example shows how to configure the SXP peer connection on SwitchB:

```plaintext
feature cts
ccts role-based enforcement
ccts sxp enable
ccts sxp connection peer 10.10.1.1 password required A2BsxpPW mode speaker
```

The following example shows how to configure the SXP peer connection on SwitchC:

```plaintext
feature cts
ccts role-based enforcement
ccts sxp enable
ccts sxp connection peer 10.10.1.1 password required A2CsxpPW mode speaker
```

Additional References for Cisco TrustSec

This sections provides additional information related to implementing Cisco TrustSec.

Related Documentation

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS licensing</td>
<td>Cisco NX-OS Licensing Guide</td>
</tr>
</tbody>
</table>
Feature History for Cisco TrustSec

This table lists the release history for this feature.

Table 13: Feature History for Cisco TrustSec

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco TrustSec</td>
<td>6.1(1)</td>
<td>Removed the requirement for the Advanced Services license.</td>
</tr>
<tr>
<td>Cisco TrustSec</td>
<td>6.1(1)</td>
<td>Added MACsec support for 40G and 100G M2 Series modules.</td>
</tr>
<tr>
<td>Cisco TrustSec</td>
<td>5.2(1)</td>
<td>Supports pause frame encryption and decryption on interfaces.</td>
</tr>
<tr>
<td>SGACL policies</td>
<td>5.0(2)</td>
<td>Supports the enabling or disabling of RBACL logging.</td>
</tr>
<tr>
<td>SGACL policies</td>
<td>5.0(2)</td>
<td>Supports the enabling, disabling, monitoring, and clearing of RBACL statistics.</td>
</tr>
<tr>
<td>Cisco TrustSec</td>
<td>4.2(1)</td>
<td>No change from Release 4.1.</td>
</tr>
</tbody>
</table>
Configuring Access Control Lists

This chapter contains the following sections:

- Information About ACLs, on page 149
- Configuring IP ACLs, on page 157
- Configuring Object Groups, on page 164
- Configuring MAC ACLs, on page 168
- Example Configuration for MAC ACLs, on page 172
- Information About VLAN ACLs, on page 172
- Configuring VACLs, on page 173
- Configuration Examples for VACL, on page 175
- Configuring ACLs on Virtual Terminal Lines, on page 176
- Configuring the ACL Resource Usage Threshold, on page 178

Information About ACLs

An access control list (ACL) is an ordered set of rules that you can use to filter traffic. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When the switch determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether the packet is permitted or denied. If there is no match, the switch applies the applicable default rule. The switch continues processing packets that are permitted and drops packets that are denied.

You can use ACLs to protect networks and specific hosts from unnecessary or unwanted traffic. For example, you could use ACLs to disallow HTTP traffic from a high-security network to the Internet. You could also use ACLs to allow HTTP traffic but only to specific sites, using the IP address of the site to identify it in an IP ACL.

IP ACL Types and Applications

The Cisco Nexus device supports IPv4 for security traffic filtering. The switch allows you to use IP access control lists (ACLs) as port ACLs, VLAN ACLs, and Router ACLs as shown in the following table.
Table 14: Security ACL Applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Supported Interfaces</th>
<th>Types of ACLs Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port ACL</td>
<td>An ACL is considered a port ACL when you apply it to one of the following: • Ethernet interface • Ethernet port-channel interface When a port ACL is applied to a trunk port, the ACL filters traffic on all VLANs on the trunk port.</td>
<td>IPv4 ACLs IPv6 ACLs</td>
</tr>
<tr>
<td>Router ACL</td>
<td>• VLAN interfaces Note You must enable VLAN interfaces globally before you can configure a VLAN interface. • Physical Layer 3 interfaces • Layer 3 Ethernet subinterfaces • Layer 3 Ethernet port-channel interfaces • Layer 3 Ethernet port-channel subinterfaces • Tunnels • Management interfaces</td>
<td>IPv4 ACLs IPv6 ACLs</td>
</tr>
<tr>
<td>VLAN ACL (VACL)</td>
<td>An ACL is a VACL when you use an access map to associate the ACL with an action and then apply the map to a VLAN.</td>
<td>IPv4 ACLs</td>
</tr>
<tr>
<td>VTY ACL</td>
<td>VTYs</td>
<td>IPv4 ACLs IPv6 ACLs</td>
</tr>
</tbody>
</table>

Application Order

When the device processes a packet, it determines the forwarding path of the packet. The path determines which ACLs that the device applies to the traffic. The device applies the ACLs in the following order:

1. Port ACL
2. Ingress VACL
3. Ingress Router ACL
4. Egress Router ACL
5. Egress VACL
Rules

Rules are what you create, modify, and remove when you configure how an ACL filters network traffic. Rules appear in the running configuration. When you apply an ACL to an interface or change a rule within an ACL that is already applied to an interface, the supervisor module creates ACL entries from the rules in the running configuration and sends those ACL entries to the applicable I/O module. Depending upon how you configure the ACL, there may be more ACL entries than rules, especially if you implement policy-based ACLs by using object groups when you configure rules.

The device allows traffic that matches the criteria in a permit rule and blocks traffic that matches the criteria in a deny rule. You have many options for configuring the criteria that traffic must meet in order to match the rule.

This section describes some of the options that you can use when you configure a rule.

Source and Destination

In each rule, you specify the source and the destination of the traffic that matches the rule. You can specify both the source and destination as a specific host, a network or group of hosts, or any host.

Protocols

IPv4, IPv6, and MAC ACLs allow you to identify traffic by protocol. For your convenience, you can specify some protocols by name. For example, in an IPv4 ACL, you can specify ICMP by name.

You can specify any protocol by the integer that represents the Internet protocol number.

Implicit Rules

IP and MAC ACLs have implicit rules, which means that although these rules do not appear in the running configuration, the switch applies them to traffic when no other rules in an ACL match.

All IPv4 ACLs include the following implicit rule:

deny ip any any

This implicit rule ensures that the switch denies unmatched IP traffic.

All IPv6 ACLs include the following implicit rule:

deny ipv6 any any

permit icmp any any nd-na
permit icmp any any nd-ns
permit icmp any any router-advertisement
permit icmp any any router-solicitation

Unless you configure an IPv6 ACL with a rule that denies ICMPv6 neighbor discovery messages, the first four rules ensure that the device permits neighbor discovery advertisement and solicitation messages. The fifth rule ensures that the device denies unmatched IPv6 traffic.

Note

If you explicitly configure an IPv6 ACL with a `deny ipv6 any any` rule, the implicit permit rules can never permit traffic. If you explicitly configure a `deny ipv6 any any` rule but want to permit ICMPv6 neighbor discovery messages, explicitly configure a rule for all five implicit rules.
All MAC ACLs include the following implicit rule:

deny any any protocol

This implicit rule ensures that the device denies the unmatched traffic, regardless of the protocol specified in the Layer 2 header of the traffic.

**Additional Filtering Options**

You can identify traffic by using additional options. IPv4 ACLs support the following additional filtering options:

- Layer 4 protocol
- TCP and UDP ports
- ICMP types and codes
- IGMP types
- Precedence level
- Differentiated Services Code Point (DSCP) value
- TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
- Established TCP connections

MAC ACLs support the following additional filtering options:

- Layer 3 protocol
- VLAN ID
- Class of Service (CoS)

**Sequence Numbers**

The Cisco Nexus device supports sequence numbers for rules. Every rule that you enter receives a sequence number, either assigned by you or assigned automatically by the device. Sequence numbers simplify the following ACL tasks:

- Adding new rules between existing rules—By specifying the sequence number, you specify where in the ACL a new rule should be positioned. For example, if you need to insert a rule between rules numbered 100 and 110, you could assign a sequence number of 105 to the new rule.

- Removing a rule—Without using a sequence number, removing a rule requires that you enter the whole rule, as follows:

  ```
  switch(config-acl)# no permit tcp 10.0.0.0/8 any
  ```

  However, if the same rule had a sequence number of 101, removing the rule requires only the following command:

  ```
  switch(config-acl)# no 101
  ```

- Moving a rule—With sequence numbers, if you need to move a rule to a different position within an ACL, you can add a second instance of the rule using the sequence number that positions it correctly, and then you can remove the original instance of the rule. This action allows you to move the rule without disrupting traffic.
If you enter a rule without a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule to the rule. For example, if the last rule in an ACL has a sequence number of 225 and you add a rule without a sequence number, the device assigns the sequence number 235 to the new rule.

In addition, the device allows you to reassign sequence numbers to rules in an ACL. Resequecing is useful when an ACL has rules numbered contiguously, such as 100 and 101, and you need to insert one or more rules between those rules.

Logical Operators and Logical Operation Units

IP ACL rules for TCP and UDP traffic can use logical operators to filter traffic based on port numbers. The Cisco Nexus device stores operator-operand couples in registers called logical operation units (LOUs) to perform operations (greater than, less than, not equal to, and range) on the TCP and UDP ports specified in an IP ACL.

Note

The range operator is inclusive of boundary values.

These LOUs minimize the number of ternary content addressable memory (TCAM) entries needed to perform these operations. A maximum of two LOUs are allowed for each feature on an interface. For example an ingress RACL can use two LOUs, and a QoS feature can use two LOUs. If an ACL feature requires more than two arithmetic operations, the first two operations use LOUs, and the remaining access control entries (ACEs) get expanded.

The following guidelines determine when the device stores operator-operand couples in LOUs:

- If the operator or operand differs from other operator-operand couples that are used in other rules, the couple is stored in an LOU.
  
  For example, the operator-operand couples "gt 10" and "gt 11" would be stored separately in half an LOU each. The couples "gt 10" and "lt 10" would also be stored separately.

- Whether the operator-operand couple is applied to a source port or a destination port in the rule affects LOU usage. Identical couples are stored separately when one of the identical couples is applied to a source port and the other couple is applied to a destination port.

  For example, if a rule applies the operator-operand couple "gt 10" to a source port and another rule applies a "gt 10" couple to a destination port, both couples would also be stored in half an LOU, resulting in the use of one whole LOU. Any additional rules using a "gt 10" couple would not result in further LOU usage.

Policy-Based ACLs

The device supports policy-based ACLs (PBACLS), which allow you to apply access control policies across object groups. An object group is a group of IP addresses or a group of TCP or UDP ports. When you create a rule, you specify the object groups rather than specifying IP addresses or ports.

Using object groups when you configure IPv4 or IPv6 ACLs can help reduce the complexity of updating ACLs when you need to add or remove addresses or ports from the source or destination of rules. For example, if three rules reference the same IP address group object, you can add an IP address to the object instead of changing all three rules.
PBACLs do not reduce the resources required by an ACL when you apply it to an interface. When you apply a PBACL or update a PBACL that is already applied, the device expands each rule that refers to object groups into one ACL entry per object within the group. If a rule specifies the source and destination both with object groups, the number of ACL entries created on the I/O module when you apply the PBACL is equal to the number of objects in the source group multiplied by the number of objects in the destination group.

The following object group types apply to port, router, and VLAN ACLs:

IPv4 address object groups
Can be used with IPv4 ACL rules to specify source or destination addresses. When you use the `permit` or `deny` command to configure a rule, the `addrgroup` keyword allows you to specify an object group for the source or destination.

IPv6 address object groups
Can be used with IPv6 ACL rules to specify source or destination addresses. When you use the `permit` or `deny` command to configure a rule, the `addrgroup` keyword allows you to specify an object group for the source or destination.

Protocol port object groups
Can be used with IPv4 and IPv6 TCP and UDP rules to specify source or destination ports. When you use the `permit` or `deny` command to configure a rule, the `portgroup` keyword allows you to specify an object group for the source or destination.

ACL Resource Management

Understanding the ACL capacities when configuring ACLs helps avoid resource contention and exhaustion. Because the platform enforces several types of ACLs in hardware rather than in software, the switch programs hardware lookup tables and various hardware resources so that when a packet arrives, the switch can perform a hardware table lookup and execute the appropriate action without affecting performance, while the packets are cut-through switched.

For typical configurations, the switch uses one of the following main hardware resources:

- Logical operation units (LOUs)-Registers that are used to store Layer 2, Layer 3, and Layer 4 operations information.
- Value, Mask, Result (VMR)-Entries in the TCAM that consist of a value pattern, the associated mask value, and a result for lookups returning a hit for the entry.

The switch optimizes the use of these hardware resources for Layer 4 operations (L4Op). When the number of L4Ops are exhausted, an ACL that needs to check a particular value using a L4Op can be expanded to use a set of entries in the TCAM instead. The ACL uses the TCAM entries to perform the same filtering that L4Op would have performed.

If the number of L4Ops are not exhausted, the switch computes the cost of using each resource. If the cost of using a set of expanded TCAM entries is less than that of using a L4Op, the switch expands the set of TCAM entries to preserve the L4Op for higher priority operations.

Depending on the size of ACL TCAM, and the size of various regions in the TCAM, it is possible that policies that are expanded might not fit within the available space. For example, after the switch is reloaded, the set of policies that were expanded before might not be expanded again.

To manage this issue, you can configure a threshold value. The threshold value is from 0 to 32 and the default value is 5. When an ACL policy needs a L4Op, the policy is expanded to check if the number of expanded TCAM entries needed exceeds the threshold value. If the number exceeds the threshold value, the expansion...
is not used, and L4Op is used instead. If the number of TCAM entries do not exceed the threshold value (that is, they are less than or equal to the threshold value), then the expanded TCAM entries are installed.

---

**Note**

If there is an ACL policy that uses both a source L4Op and destination L4Op, the source L4Op and destination L4Op are expanded individually. The following example shows an ACL policy with source and destination L4Ops:

```
permit tcp any get 546 any range 236 981
```

---

### Statistics and ACLs

The device can maintain global statistics for each rule that you configure in IPv4, IPv6, and MAC ACLs. If an ACL is applied to multiple interfaces, the maintained rule statistics are the sum of packet matches (hits) on all the interfaces on which that ACL is applied.

---

**Note**

The device does not support interface-level ACL statistics.

For each ACL that you configure, you can specify whether the device maintains statistics for that ACL, which allows you to turn ACL statistics on or off as needed to monitor traffic filtered by an ACL or to help troubleshoot the configuration of an ACL.

The device does not maintain statistics for implicit rules in an ACL. For example, the device does not maintain a count of packets that match the implicit *deny ip any any* rule at the end of all IPv4 ACLs. If you want to maintain statistics for implicit rules, you must explicitly configure the ACL with rules that are identical to the implicit rules.

### Licensing Requirements for ACLs

The following table shows the licensing requirements for this feature:

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>No license is required to use ACLs.</td>
</tr>
</tbody>
</table>

### Prerequisites for ACLs

IP ACLs have the following prerequisites:

- You must be familiar with IP addressing and protocols to configure IP ACLs.
- You must be familiar with the interface types that you want to configure with ACLs.

VACLs have the following prerequisite:

- Ensure that the IP ACL that you want to use in the VACL exists and is configured to filter traffic in the manner that you need for this application.
Guidelines and Limitations for ACLs

IP ACLs have the following configuration guidelines and limitations:

- We recommend that you perform ACL configuration using the Session Manager. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. This is especially useful for ACLs that include more than about 1000 rules.

- To apply an IP ACL to a VLAN interface, you must have enabled VLAN interfaces globally.

MAC ACLs have the following configuration guidelines and limitations:

- MAC ACLs apply to ingress traffic only.

- ACL statistics are not supported if the DHCP snooping feature is enabled.

VACLs have the following configuration guidelines and limitations:

- We recommend that you perform ACL configurations using the Session Manager. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration.

- ACL statistics are not supported if the DHCP snooping feature is enabled.

Default ACL Settings

The following table lists the default settings for IP ACLs parameters.

Table 15: Default IP ACLs Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP ACLs</td>
<td>No IP ACLs exist by default.</td>
</tr>
<tr>
<td>ACL rules</td>
<td>Implicit rules apply to all ACLs.</td>
</tr>
<tr>
<td>Object groups</td>
<td>No object groups exist by default.</td>
</tr>
</tbody>
</table>

The following table lists the default settings for VACL parameters.

Table 16: Default VACL Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>VACLs</td>
<td>No IP ACLs exist by default.</td>
</tr>
<tr>
<td>ACL rules</td>
<td>Implicit rules apply to all ACLs.</td>
</tr>
</tbody>
</table>
Configuring IP ACLs

Creating an IP ACL

You can create an IPv4 or IPv6 ACL on the switch and add rules to it.

Procedure

Step 1  
switch# configure terminal
Enters global configuration mode.

Step 2  
switch(config)# {ip | ipv6} access-list name
Creates the IP ACL and enters IP ACL configuration mode. The name argument can be up to 64 characters.

Step 3  
switch(config-acl)# [sequence-number] {permit | deny} protocol source destination
Creates a rule in the IP ACL. You can create many rules. The sequence-number argument can be a whole number between 1 and 4294967295.

The permit and deny commands support many ways of identifying traffic. For more information, see the Command Reference for the specific Cisco Nexus device.

Step 4  
(Optional) switch(config-acl)# statistics
Specifies that the switch maintains global statistics for packets that match the rules in the ACL.

Step 5  
(Optional) switch# show {ip | ipv6} access-lists name
Displays the IP ACL configuration.

Step 6  
(Optional) switch# copy running-config startup-config
Copies the running configuration to the startup configuration.

Example

This example shows how to create an IPv4 ACL:

switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# statistics

This example shows how to create an IPv6 ACL:

switch# configure terminal
switch(config)# ipv6 access-list acl-01-ipv6
switch(config-ipv6-acl)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
Changing an IP ACL

You can add and remove rules in an existing IPv4 or IPv6 ACL. You cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes.

If you need to add more rules between existing rules than the current sequence numbering allows, you can use the `resequence` command to reassign sequence numbers.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> switch(config)# {ip</td>
<td>ipv6} access-list name</td>
</tr>
<tr>
<td><strong>Step 3</strong> switch(config)# ip access-list name</td>
<td>Enters IP ACL configuration mode for the ACL that you specify by name.</td>
</tr>
<tr>
<td><strong>Step 4</strong> switch(config-acl)# [sequence-number] {permit</td>
<td>deny} protocol source destination</td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) switch(config-acl)# no {sequence-number</td>
<td>{permit</td>
</tr>
<tr>
<td><strong>Step 6</strong> (Optional) switch(config-acl)# [no] statistics</td>
<td>Specifies that the switch maintains global statistics for packets that match the rules in the ACL. The <code>no</code> option stops the switch from maintaining global statistics for the ACL.</td>
</tr>
<tr>
<td><strong>Step 7</strong> (Optional) switch# show ip access-lists name</td>
<td>Displays the IP ACL configuration.</td>
</tr>
<tr>
<td><strong>Step 8</strong> (Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

### Related Topics
- [Changing Sequence Numbers in an IP ACL](#), on page 159
Removing an IP ACL

You can remove an IP ACL from the switch.

Before you remove an IP ACL from the switch, be sure that you know whether the ACL is applied to an interface. The switch allows you to remove ACLs that are currently applied. Removing an ACL does not affect the configuration of interfaces where you have applied the ACL. Instead, the switch considers the removed ACL to be empty.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 switch(config)# no {ip</td>
<td>ipv6} access-list name</td>
</tr>
<tr>
<td>Step 3 switch(config)# no ip access-list name</td>
<td>Removes the IP ACL that you specified by name from the running configuration.</td>
</tr>
<tr>
<td>Step 4 (Optional) switch# show running-config</td>
<td>Displays the ACL configuration. The removed IP ACL should not appear.</td>
</tr>
<tr>
<td>Step 5 (Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Changing Sequence Numbers in an IP ACL

You can change all the sequence numbers assigned to the rules in an IP ACL.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 (Optional) switch# show {ip</td>
<td>ipv6} access-lists name</td>
</tr>
<tr>
<td>Step 3 (Optional) switch# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Configuring ACLs with Logging

You can create an access-control list for logging traffic of a specified protocol and address.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>switch(config)# `{ip</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switch(config-acl)# <code>permit protocol source destination log</code>&lt;br&gt;Creates a rule to log traffic of the specified protocol in the syslog file. in the IP ACL. Valid values for the <code>protocol</code> argument are:&lt;br&gt;• <code>icmp</code>—ICMP&lt;br&gt;• <code>igmp</code>—IGMP&lt;br&gt;• <code>ip</code>—IPv4&lt;br&gt;• <code>ipv6</code>—IPv6&lt;br&gt;• <code>tcp</code>—TCP&lt;br&gt;• <code>udp</code>—UDP&lt;br&gt;• <code>sctp</code>—SCTP (IPv6 only)&lt;br&gt;The source and destination arguments can be the IP address with a network wildcard (IPv4 only), IP address and variable-length subnet mask, host address, or <code>any</code> to designate any address. For more information, see the System Management configuration guide and the Security command reference for your platform.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>switch(config-acl)# <code>exit</code>&lt;br&gt;Exists the current configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) switch(config)# <code>copy running-config startup-config</code>&lt;br&gt;Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to create an ACL for logging entries that match IPv4 TCP traffic from any source and any destination:

```
switch# configuration terminal
switch(config)# ip access-list tcp_log
switch(config-acl)# permit tcp any any log
switch(config-acl)# exit
switch(config)# copy running-config startup-config
```

**Applying an IP ACL to mgmt0**

You can apply an IPv4 or IPv6 ACL to the management interface (mgmt0).
Before you begin

Ensure that the ACL that you want to apply exists and that it is configured to filter traffic in the manner that you need for this application.

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>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</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>interface mgmt port</td>
<td>Enters configuration mode for the management interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# interface mgmt0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)#</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>ip access-group access-list {in</td>
<td>out}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)#ip access-group acl-120</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)#out</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>(Optional) show running-config aclmgr</td>
<td>Displays the ACL configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)#show running-config aclmgr</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>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)#copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- Creating an IP ACL

Applying an IP ACL as a Router ACL

You can apply an IPv4 or IPv6 ACL to any of the following types of interfaces:

- Physical Layer 3 interfaces and subinterfaces
- Layer 3 Ethernet port-channel interfaces and subinterfaces
- VLAN interfaces
- Tunnels
- Management interfaces
Before you begin

Ensure that the ACL you want to apply exists and that it is configured to filter traffic in the manner that you need for this application.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 Enter one of the following commands:</td>
<td>Enters configuration mode for the interface type that you specified.</td>
</tr>
<tr>
<td>- switch(config)# interface ethernet slot/port[. number]</td>
<td></td>
</tr>
<tr>
<td>- switch(config)# interface port-channel channel-number[. number]</td>
<td></td>
</tr>
<tr>
<td>- switch(config)# interface tunnel tunnel-number</td>
<td></td>
</tr>
<tr>
<td>- switch(config)# interface vlan vlan-ID</td>
<td></td>
</tr>
<tr>
<td>- switch(config)# interface mgmt port</td>
<td></td>
</tr>
<tr>
<td>Step 3 Enter one of the following commands:</td>
<td>Applies an IPv4 or IPv6 ACL to the Layer 3 interface for traffic flowing in the direction specified. You can apply one router ACL per direction.</td>
</tr>
<tr>
<td>- switch(config-if)# ip access-group access-list {in</td>
<td>out}</td>
</tr>
<tr>
<td>- switch(config-if)# ipv6 traffic-filter access-list {in</td>
<td>out}</td>
</tr>
<tr>
<td>Step 4 (Optional) switch(config-if)# show running-config aclmgr</td>
<td>Displays the ACL configuration.</td>
</tr>
<tr>
<td>Step 5 (Optional) switch(config-if)# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Applying an IP ACL as a Port ACL

You can apply an IPv4 ACL to a physical Ethernet interface or a PortChannel. ACLs applied to these interface types are considered port ACLs.

Note

Some configuration parameters when applied to an PortChannel are not reflected on the configuration of the member ports.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Verifying IP ACL Configurations

To display IP ACL information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Displays ACL configuration, including IP ACL configuration and interfaces that IP ACLs are applied to.</td>
</tr>
<tr>
<td>show running-config interface</td>
<td>Displays the configuration of an interface to which you have applied an ACL.</td>
</tr>
</tbody>
</table>

For detailed information about the fields in the output from these commands, refer to the Command Reference for your Cisco Nexus device.

### Monitoring and Clearing IP ACL Statistics

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show {ip</td>
<td>ipv6} access-lists name</td>
</tr>
<tr>
<td>show ip access-lists name</td>
<td>Displays IP ACL configuration. If the IP ACL includes the statistics command, then the show ip access-lists command output includes the number of packets that have matched each rule.</td>
</tr>
<tr>
<td>clear {ip</td>
<td>ipv6} access-list counters [access-list-name]</td>
</tr>
<tr>
<td>clear ip access-list counters [access-list-name]</td>
<td>Clears statistics for all IP ACLs or for a specific IP ACL.</td>
</tr>
</tbody>
</table>
Configuring Object Groups

You can use object groups to specify source and destination addresses and protocol ports in IPv4 ACL and IPv6 ACL rules.

Session Manager Support for Object Groups

Session Manager supports the configuration of object groups. This feature allows you to create a configuration session and verify your object group configuration changes prior to committing them to the running configuration. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.

Creating and Changing an IPv4 Address Object Group

You can create and change an IPv4 address group object.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>object-group ip address name</td>
<td>Creates the IPv4 address object group and enters IPv4 address object-group configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# object-group ip address ipv4-addr-group-13</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter one of the following commands:</td>
<td>Creates an entry in the object group. For each entry that you want to create, use the <code>host</code> command and specify a single host or omit the <code>host</code> command to specify a network of hosts.</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-ipaddr-ogroup)# host 10.99.32.6</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter one of the following commands:</td>
<td>Removes an entry in the object group. For each entry that you want to remove from the object group, use the <code>no</code> form of the <code>host</code> command.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Creating and Changing an IPv6 Address Object Group

You can create and change an IPv6 address group object.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> config t</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: switch# config t switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> object-group ipv6 address name</td>
<td>Creates the IPv6 address object group and enters IPv6 address object-group configuration mode.</td>
</tr>
<tr>
<td>Example: switch(config)# object-group ipv6 address ipv6-addr-group-A7 switch(config-ipv6addr-ogroup)#</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 3** Enter one of the following commands:  
  - [sequence-number] host IPv6-address  
  - [sequence-number] IPv6-address/prefix-len | Creates an entry in the object group. For each entry that you want to create, use the **host** command and specify a single host or omit the **host** command specify a network of hosts. |
| Example: switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1 | |
| **Step 4** Enter one of the following commands:  
  - no sequence-number  
  - no host IPv6-address  
  - no IPv6-address/prefix-len | Removes an entry from the object group. For each entry that you want to remove from the object group, use the **no** form of the **host** command. |

---

### Purpose

**Command or Action**

**Example:**

switch(config-ipaddr-ogroup)# no host 10.99.32.6

**Step 5** *(Optional)* **show object-group name**

**Example:**

switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13

**Step 6** *(Optional)* **copy running-config startup-config**

**Example:**

switch(config-ipaddr-ogroup)# copy running-config startup-config
## Creating and Changing a Protocol Port Object Group

You can create and change a protocol port object group.

### 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>
</tbody>
</table>
| Example: | `switch# configure terminal`  
`switch(config)#` | |
| **Step 2** | `object-group ip port name` | Creates the protocol port object group and enters port object-group configuration mode. |
| Example: | `switch(config)# object-group ip port`  
`NYC-datacenter-ports`  
`switch(config-port-ogroup)#` | |
| **Step 3** | `[sequence-number] operator port-number`  
`[port-number]` | Creates an entry in the object group. For each entry that you want to create, use one of the following operator commands: |
| Example: | `switch(config-port-ogroup)# eq 80` | - **eq**—Matches the port number that you specify only.  
- **gt**—Matches port numbers that are greater than (and not equal to) the port number that you specify.  
- **lt**—Matches port numbers that are less than (and not equal to) the port number that you specify. |
Purpose

- **neq**—Matches all port numbers except for the port number that you specify.
- **range**—Matches the range of port number between and including the two port numbers that you specify.

**Note**  
The `range` command is the only operator command that requires two `port-number` arguments.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 4**  
no `{sequence-number | operator port-number [port-number]}  
Example:  
switch(config-port-oigroup)# no eq 80               | Removes an entry from the object group. For each entry that you want to remove, use the no form of the applicable operator command. |
| **Step 5**  
(Optional) **show object-group name**  
Example:  
switch(config-port-oigroup)# show object-group NYC-datacenter-ports | Displays the object group configuration.                                                        |
| **Step 6**  
(Optional) **copy running-config startup-config**  
Example:  
switch(config-port-oigroup)# copy running-config startup-config | Copies the running configuration to the startup configuration.                                |

## Removing an Object Group

You can remove an IPv4 address object group, an IPv6 address object group, or a protocol port object group.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
configure terminal  
Example:  
switch# configure terminal  
switch(config)# | Enters global configuration mode.                                                             |
| **Step 2**  
no object-group `{ip address | ipv6 address | ip port} name  
Example:  
switch(config)# no object-group ip address_ipv4-addr-group-A7 | Removes the object group that you specified.                                                   |
Verifying the Object-Group Configuration

To display object-group configuration information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show object-group</td>
<td>Displays the object-group configuration.</td>
</tr>
<tr>
<td>show running-config aclmgr</td>
<td>Displays ACL configuration, including object groups.</td>
</tr>
</tbody>
</table>

For detailed information about the fields in the output from these commands, see the Cisco Nexus 7000 Series NX-OS Security Command Reference.

Configuring MAC ACLs

Creating a MAC ACL

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 switch# mac access-list name</td>
<td>Creates the MAC ACL and enters ACL configuration mode.</td>
</tr>
<tr>
<td>Step 3 switch(config-mac-acl)# [sequence-number] {permit</td>
<td>deny} source destination protocol</td>
</tr>
<tr>
<td>Step 4 (Optional) switch(config-mac-acl)# statistics</td>
<td>Specifies that the switch maintains global statistics for packets matching the rules in the ACL.</td>
</tr>
</tbody>
</table>
### Changing a MAC ACL

In an existing MAC ACL, you can add and remove rules. You cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes.

If you need to add more rules between existing rules than the current sequence numbering allows, you can use the `resequence` command to reassign sequence numbers.

#### 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>switch# <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>switch(config)# <code>mac access-list name</code></td>
<td>Enters ACL configuration mode for the ACL that you specify by name.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switch(config-mac-acl)# `[sequence-number] [permit</td>
<td>deny] source destination protocol`</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) switch(config-mac-acl)# `no [sequence-number] [permit</td>
<td>deny] source destination protocol`</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) switch(config-mac-acl)# <code>[no] statistics</code></td>
<td>Specifies that the switch maintains global statistics for packets matching the rules in the ACL. The <code>no</code> option stops the switch from maintaining global statistics for the ACL.</td>
</tr>
</tbody>
</table>
Removing a MAC ACL

You can remove a MAC ACL from the switch.

Be sure that you know whether the ACL is applied to an interface. The switch allows you to remove ACLs that are currently applied. Removing an ACL does not affect the configuration of interfaces where you have applied the ACL. Instead, the switch considers the removed ACL to be empty.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# no mac access-list name</td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) switch# show mac access-lists</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) switch# copy running-config</td>
</tr>
</tbody>
</table>

Changing Sequence Numbers in a MAC ACL

You can change all the sequence numbers assigned to rules in a MAC ACL. Resequencing is useful when you need to insert rules into an ACL and there are not enough available sequence numbers.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
</tr>
</tbody>
</table>
Applying a MAC ACL as a Port ACL

You can apply a MAC ACL as a port ACL to any of the following interface types:

- Ethernet interfaces
- EtherChannel interfaces

Be sure that the ACL that you want to apply exists and is configured to filter traffic as necessary for this application.

Some configuration parameters when applied to an EtherChannel are not reflected on the configuration of the member ports.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>switch(config)# interface {ethernet [chassis/]slot/port</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switch(config-if)# mac port access-group access-list</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) switch# show running-config</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>
Related Topics
Creating an IP ACL, on page 157

Verifying MAC ACL Configurations

To display MAC ACL information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mac access-lists</td>
<td>Displays the MAC ACL configuration.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays ACL configuration, including MAC ACLs and the interfaces that</td>
</tr>
<tr>
<td></td>
<td>ACLs are applied to.</td>
</tr>
<tr>
<td>show running-config interface</td>
<td>Displays the configuration of the interface to which you applied the</td>
</tr>
<tr>
<td></td>
<td>ACL.</td>
</tr>
</tbody>
</table>

Displaying and Clearing MAC ACL Statistics

To display and clear MAC ACL statistics, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mac access-lists</td>
<td>Displays MAC ACL configuration. If the MAC ACL includes the statistics</td>
</tr>
<tr>
<td></td>
<td>command, the show mac access-lists command output includes the number</td>
</tr>
<tr>
<td></td>
<td>of packets that have matched each rule.</td>
</tr>
<tr>
<td>clear mac access-list counters</td>
<td>Clears statistics for all MAC ACLs or for a specific MAC ACL.</td>
</tr>
</tbody>
</table>

Example Configuration for MAC ACLs

This example shows how to create a MAC ACL named acl-mac-01 and apply it to Ethernet interface 1/1:

```
switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any
switch(config-mac-acl)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# mac access-group acl-mac-01
```

Information About VLAN ACLs

A VLAN ACL (VAACL) is one application of an IP ACL. You can configure VAACLs to apply to all packets that are bridged within a VLAN. VAACLs are used strictly for security packet filtering. VAACLs are not defined by direction (ingress or egress).
VACLs and Access Maps

VACLs use access maps to link an IP ACL to an action. The switch takes the configured action on packets that are permitted by the VACL.

VACLs and Actions

In access map configuration mode, you use the `action` command to specify one of the following actions:

- **Forward**—Sends the traffic to the destination determined by normal operation of the switch.
- **Drop**—Drops the traffic.

Statistics

The Cisco Nexus device can maintain global statistics for each rule in a VACL. If a VACL is applied to multiple VLANs, the maintained rule statistics are the sum of packet matches (hits) on all the interfaces on which that VACL is applied.

*Note*

The Cisco Nexus device does not support interface-level VACL statistics.

For each VLAN access map that you configure, you can specify whether the switch maintains statistics for that VACL. This allows you to turn VACL statistics on or off as needed to monitor traffic filtered by a VACL or to help troubleshoot VLAN access-map configuration.

Configuring VACLs

Creating or Changing a VACL

You can create or change a VACL. Creating a VACL includes creating an access map that associates an IP ACL with an action to be applied to the matching traffic.

**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>switch# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>switch(config)# vlan access-map map-name</code></td>
<td>Enters access map configuration mode for the access map specified.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>switch(config-access-map)# match ip address ip-access-list</code></td>
<td>Specifies an IPv4 and IPv6 ACL for the map.</td>
</tr>
<tr>
<td>Step 4</td>
<td>`switch(config-access-map)# action {drop</td>
<td>forward}`</td>
</tr>
</tbody>
</table>
Removing a VACL

You can remove a VACL, which means that you will delete the VLAN access map.

Be sure that you know whether the VACL is applied to a VLAN. The switch allows you to remove VACLs that are currently applied. Removing a VACL does not affect the configuration of VLANs where you have applied the VACL. Instead, the switch considers the removed VACL to be empty.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 switch(config)# no vlan access-map map-name</td>
<td>Removes the VLAN access map configuration for the specified access map.</td>
</tr>
<tr>
<td>Step 3 (Optional) switch(config)# show running-config</td>
<td>Displays ACL configuration.</td>
</tr>
<tr>
<td>Step 4 (Optional) switch(config)# copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

Applying a VACL to a VLAN

You can apply a VACL to a VLAN.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 switch(config)# [no] vlan filter map-name vlan-list list</td>
<td>Applies the VACL to the VLANs by the list that you specified. The no option unapplies the VACL.</td>
</tr>
</tbody>
</table>
The `vlan-list` command can specify a list of up to 32 VLANs, but multiple `vlan-list` commands can be configured to cover more than 32 VLANs.

**Step 3**
(Optional) `switch(config)# show running-config`

Displays ACL configuration.

**Step 4**
(Optional) `switch(config)# copy running-config startup-config`

Copies the running configuration to the startup configuration.

### Verifying the VACL Configuration

To display VACL configuration information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config aclmgr</code></td>
<td>Displays ACL configuration, including VACL-related configuration.</td>
</tr>
<tr>
<td><code>show vlan filter</code></td>
<td>Displays information about VACLs that are applied to a VLAN.</td>
</tr>
<tr>
<td><code>show vlan access-map</code></td>
<td>Displays information about VLAN access maps.</td>
</tr>
</tbody>
</table>

### Displaying and Clearing VACL Statistics

To display or clear VACL statistics, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show vlan access-list</code></td>
<td>Displays VACL configuration. If the VLAN access-map includes the <code>statistics</code> command, then the <code>show vlan access-list</code> command output includes the number of packets that have matched each rule.</td>
</tr>
<tr>
<td><code>clear vlan access-list counters</code></td>
<td>Clears statistics for all VACLs or for a specific VACL.</td>
</tr>
</tbody>
</table>

### Configuration Examples for VACL

The following example shows how to configure a VACL to forward traffic permitted by an IP ACL named acl-ip-01 and how to apply the VACL to VLANs 50 through 82:

```
switch# configure terminal
switch(config)# vlan access-map acl-ip-map
switch(config-access-map)# match ip address acl-ip-01
switch(config-access-map)# action forward
switch(config-access-map)# exit
```
Configuring ACLs on Virtual Terminal Lines

To restrict incoming and outgoing connections for IPv4 or IPv6 between a Virtual Terminal (VTY) line and the addresses in an access list, use the `access-class` command in line configuration mode. To remove access restrictions, use the `no` form of this command.

Follow these guidelines when configuring ACLs on VTY lines:

- Set identical restrictions on all VTY lines because a user can connect to any of them.
- Statistics per entry is not supported for ACLs on VTY lines.

**Before you begin**

Be sure that the ACL that you want to apply exists and is configured to filter traffic for this application.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>switch(config)# line vty</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config)# line vty switch(config-line)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switch(config-line)# access-class access-list-number {in</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-line)# access-class ozi2 in switch(config-line)# access-class ozi3 out switch(config)#</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) switch(config-line)# no access-class access-list-number {in</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-line)# no access-class ozi2 in switch(config-line)# no access-class ozi3 out switch(config)#</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>switch(config-line)# exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch(config-line)# exit switch#</td>
</tr>
</tbody>
</table>
### Purpose

#### Command or Action

<table>
<thead>
<tr>
<th>Step 6</th>
<th>(Optional) switch# show running-config aclmgr</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>switch# show running-config aclmgr</td>
</tr>
</tbody>
</table>

#### Command or Action

<table>
<thead>
<tr>
<th>Step 7</th>
<th>(Optional) switch# copy running-config startup-config</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>

### Example

The following example shows how to apply the access-class ozi2 command to the in-direction of the vty line.

```con
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# line vty
switch(config-line)# access-class ozi2 in
switch(config-line)# exit
switch#
```

### Verifying ACLs on VTY Lines

To display the ACL configurations on VTY lines, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config aclmgr</td>
<td>Displays the running configuration of the ACLs configured on the switch.</td>
</tr>
<tr>
<td>show users</td>
<td>Displays the users that are connected.</td>
</tr>
<tr>
<td>show access-lists access-list-name</td>
<td>Display the statistics per entry.</td>
</tr>
</tbody>
</table>

### Configuration Examples for ACLs on VTY Lines

The following example shows the connected users on the console line (ttyS0) and the VTY lines (pts/0 and pts/1).

```con
switch# show users
NAME   LINE     TIME       IDLE      PID   COMMENT
admin  ttyS0   Aug 27 20:45  .        14425 *
admin  pts/0   Aug 27 20:06  00:46   14176 (172.18.217.82) session=ssh
admin  pts/1   Aug 27 20:52   .       14584 (10.55.144.118)       
```

The following example shows how to allow vty connections to all IPv4 hosts except 172.18.217.82 and how to deny vty connections to any IPv4 host except 10.55.144.118, 172.18.217.79, 172.18.217.82, 172.18.217.92:
switch# show running-config aclmgr
!Time: Fri Aug 27 22:01:09 2010
version 5.0(2)N1(1)
ip access-list ozi
  10 deny ip 172.18.217.82/32 any
  20 permit ip any any
ip access-list ozi2
  10 permit ip 10.55.144.118/32 any
  20 permit ip 172.18.217.79/32 any
  30 permit ip 172.18.217.82/32 any
  40 permit ip 172.18.217.92/32 any

line vty
  access-class ozi in
  access-class ozi2 out

The following example shows how to configure the IP access list by enabling per-entry statistics for the ACL:

switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list ozi2
switch(config-acl)# statistics per-entry
switch(config-acl)# deny tcp 172.18.217.83/32 any
switch(config-acl)# exit

switch(config)# ip access-list ozi
switch(config-acl)# statistics per-entry
switch(config-acl)# permit ip 172.18.217.20/24 any
switch(config-acl)# exit

switch#

The following example shows how to apply the ACLs on VTY in and out directions:

switch(config)# line vty
switch(config-line)# ip access-class ozi in
switch(config-line)# access-class ozi2 out
switch(config-line)# exit
switch#

The following example shows how to remove the access restrictions on the VTY line:

switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# line vty
switch(config-line)# no access-class ozi2 in
switch(config-line)# no ip access-class ozi2 in
switch(config-line)# exit
switch#

Configuring the ACL Resource Usage Threshold

You can configure a threshold value for the number of Logical Operation Units (LOUs).
## 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>switch# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>switch(config)# hardware access-list lou resource threshold value</code></td>
<td>Configures the threshold value for the number of LOUs.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>(Optional) switch(config-if)# copy running-config startup-config</code></td>
<td>Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

## Example

The following example shows how to configure the maximum threshold value for LOUs:

```bash
switch# configuration terminal
switch(config)# hardware access-list lou resource threshold 15
```
CHAPTER 10

Configuring Port Security

This chapter includes the following sections:

- Information About Port Security, on page 181
- Licensing Requirements for Port Security, on page 186
- Prerequisites for Port Security, on page 186
- Guidelines and Limitations for Port Security, on page 186
- Guidelines and Limitations for Port Security on vPCs, on page 187
- Default Settings for Port Security, on page 187
- Configuring Port Security, on page 188
- Verifying the Port Security Configuration, on page 198
- Displaying Secure MAC Addresses, on page 198
- Configuration Example for Port Security, on page 198
- Configuration Example of Port Security in a vPC Domain, on page 199
- Additional References for Port Security, on page 199

Information About Port Security

Port security allows you to configure Layer 2 physical interfaces and Layer 2 port-channel interfaces to allow inbound traffic from only a restricted set of MAC addresses. The MAC addresses in the restricted set are called secure MAC addresses. In addition, the device does not allow traffic from these MAC addresses on another interface within the same VLAN. The number of MAC addresses that the device can secure is configurable per interface.

Note

Unless otherwise specified, the term interface refers to both physical interfaces and port-channel interfaces; physical interfaces, port-channel interfaces, and vPCs; likewise, the term Layer 2 interface refers to both Layer 2 physical interfaces and Layer 2 port-channel interfaces.

Secure MAC Address Learning

The process of securing a MAC address is called learning. A MAC address can be a secure MAC address on one interface only. For each interface that you enable port security on, the device can learn a limited number
of MAC addresses by the static, dynamic, or sticky methods. The way that the device stores secure MAC addresses varies depending upon how the device learned the secure MAC address.

**Static Method**

The static learning method allows you to manually add or remove secure MAC addresses to the running configuration of an interface. If you copy the running configuration to the startup configuration, static secure MAC addresses are unaffected if the device restarts.

A static secure MAC address entry remains in the configuration of an interface until one of the following events occurs:

- You explicitly remove the address from the configuration.
- You configure the interface to act as a Layer 3 interface.

Adding secure addresses by the static method is not affected by whether dynamic or sticky address learning is enabled.

**Dynamic Method**

By default, when you enable port security on an interface, you enable the dynamic learning method. With this method, the device secures MAC addresses as ingress traffic passes through the interface. If the address is not yet secured and the device has not reached any applicable maximum, it secures the address and allows the traffic.

The device stores dynamic secure MAC addresses in memory. A dynamic secure MAC address entry remains secured on an interface until one of the following events occurs:

- The device restarts.
- The interface restarts.
- The address reaches the age limit that you configured for the interface.
- You explicitly remove the address. For more information, see Removing a Dynamic Secure MAC Address, on page 194.
- You configure the interface to act as a Layer 3 interface.

**Sticky Method**

If you enable the sticky method, the device secures MAC addresses in the same manner as dynamic address learning, but the device stores addresses learned by this method in nonvolatile RAM (NVRAM). As a result, addresses learned by the sticky method persist through a device restart. Sticky secure MAC addresses do not appear in the running configuration of an interface.

Dynamic and sticky address learning are mutually exclusive. When you enable sticky learning on an interface, the device stops dynamic learning and performs sticky learning instead. If you disable sticky learning, the device resumes dynamic learning.

A sticky secure MAC address entry remains secured on an interface until one of the following events occurs:

- You explicitly remove the sticky MAC address configuration from the interface. For more information, see Removing a Sticky Secure MAC Address, on page 193.
- You configure the interface to act as a Layer 3 interface.
Dynamic Address Aging

The device ages MAC addresses learned by the dynamic method and drops them after the age limit is reached. You can configure the age limit on each interface. The range is from 1 to 1440 minutes. The default aging time is 0, which disables aging.

The method that the device uses to determine that the MAC address age is also configurable. The two methods of determining address age are as follows:

Inactivity

The length of time after the device last received a packet from the address on the applicable interface.

Absolute

The length of time after the device learned the address. This is the default aging method; however, the default aging time is 0 minutes, which disables aging.

Note

If the absolute method is used to age out a MAC address, then depending on the traffic rate, few packets may drop each time a MAC address is aged out and relearned. To avoid this use inactivity timeout.

Secure MAC Address Maximums

By default, an interface can have only one secure MAC address. You can configure the maximum number of MAC addresses permitted per interface or per VLAN on an interface. Maximums apply to secure MAC addresses learned by any method: dynamic, sticky, or static.

Note

In vPC domains, the configuration on the primary vPC takes effect.

Tip

To ensure that an attached device has the full bandwidth of the port, set the maximum number of addresses to one and configure the MAC address of the attached device.

The following three limits can determine how many secure MAC addresses are permitted on an interface:

System maximum

The device has a nonconfigurable limit of 8192 secure MAC addresses. If learning a new address would violate the device maximum, the device does not permit the new address to be learned, even if the interface or VLAN maximum has not been reached.

Interface maximum

You can configure a maximum number of 1025 secure MAC addresses for each interface protected by port security. The default interface maximum is one address. Sum of all interface maximums on a switch cannot exceed the system maximum.

VLAN maximum

You can configure the maximum number of secure MAC addresses per VLAN for each interface protected by port security. The sum of all VLAN maximums under an interface cannot exceed the configured
interface maximum. VLAN maximums are useful only for trunk ports. There are no default VLAN maximums.

You can configure VLAN and interface maximums per interface, as needed; however, when the new limit is less than the applicable number of secure addresses, you must reduce the number of secure MAC addresses first. Otherwise, the configuration of new limit is rejected.

Security Violations and Actions

Port security triggers security violations when either of the two following events occur:

MAX Count Violation

Ingress traffic arrives at an interface from a nonsecure MAC address and learning the address would exceed the applicable maximum number of secure MAC addresses.

When an interface has both a VLAN maximum and an interface maximum configured, a violation occurs when either maximum is exceeded. For example, consider the following on a single interface configured with port security:

- VLAN 1 has a maximum of 5 addresses
- The interface has a maximum of 20 addresses

The device detects a violation when any of the following occurs:

- The device has learned five addresses for VLAN 1 and inbound traffic from a sixth address arrives at the interface in VLAN 1.

MAC Move Violation

Ingress traffic from a secure MAC address arrives at a different secured interface in the same VLAN as the interface on which the address is secured.

When a security violation occurs, the device increments the security violation counter for the interface and takes the action specified by the port security configuration of the interface. If a violation occurs because ingress traffic from a secure MAC address arrives at a different interface than the interface on which the address is secure, the device applies the action on the interface that received the traffic.

The violation modes and the possible actions that a device can take are as follows:

Shutdown violation mode

Error disables the interface that received the packet triggering the violation and the port shuts down. The security violation count is set to 1. This action is the default. After you reenable the interface, it retains its port security configuration, including its static and sticky secure MAC addresses. However, the dynamic MAC addresses are not retained and have to relearned.

You can use the errdisable recovery cause pssecure-violation global configuration command to configure the device to reenable the interface automatically if a shutdown occurs, or you can manually reenable the interface by entering the shutdown and no shut down interface configuration commands. For detailed information about the commands, see the Security Command Reference for your platform.

Restrict violation mode

Drops ingress traffic from any nonsecure MAC addresses.
The device keeps a count of the number of unique source MAC addresses of dropped packets, which is called the security violation count.

Violation is triggered for each unique nonsecure source MAC address and security violation count increments till 10, which is the maximum value. The maximum value of 10 is fixed and not configurable.

Address learning continues until the maximum security violations (10 counts) have occurred on the interface. Traffic from addresses learned after the first security violation are added as BLOCKED entries in the MAC table and dropped. These BLOCKED MAC address age out after 5 minutes. The BLOCKED MAC address age out time of 5 minutes is fixed and not configurable.

Depending on the violation type, RESTRICT mode action varies as follows:

- In case of MAX count violation, after the maximum number of MAX count violations (10) is reached, the device stops learning new MAC addresses. Interface remains up.

- In case of MAC move violation, when the maximum security violations have occurred on the interface, the interface is error Disabled.

**Protect violation mode**

Prevents further violations from occurring. The address that triggered the security violation is learned but any traffic from the address is dropped. Security violation counter is set to 1, which is the maximum value. Further address learning stops. Interface remains up.

Note that the security violation is reset to 0 after the interface is recovered from violation through one of the following events:

- Dynamic secure MAC addresses age out
- Interface flap, link down, or link up events
- Port-security disable and re-enable on the interface
- Changing violation mode of the interface

---

**If an interface is errDisabled, you can bring it up only by flapping the interface.**

---

**Port Type Changes**

When you have configured port security on a Layer 2 interface and you change the port type of the interface, the device behaves as follows:

**Access port to trunk port**

When you change a Layer 2 interface from an access port to a trunk port, the device deletes all secure addresses learned by the dynamic method. The device moves the addresses learned by the static method to the native trunk VLAN. The sticky MAC addresses remain in same VLAN if the VLAN exists. Otherwise, the MAC addresses move to the native VLAN of the trunk port.

**Trunk port to access port**

When you change a Layer 2 interface from a trunk port to an access port, the device drops all secure addresses learned by the dynamic method. It also moves all addresses learned by the sticky method on
the native trunk VLAN to the access VLAN. The device drops secure addresses learned by the sticky method if they are not on the native trunk VLAN.

**Switched port to routed port**

When you change an interface from a Layer 2 interface to a Layer 3 interface, the device disables port security on the interface and discards all port security configuration for the interface. The device also discards all secure MAC addresses for the interface, regardless of the method used to learn the address.

**Routed port to switched port**

When you change an interface from a Layer 3 interface to a Layer 2 interface, the device has no port security configuration for the interface.

The static secure addresses that are configured per access or trunk VLAN on an interface are not retained during the following events:

- Changing global VLAN mode of the active VLANs on an interface between classical Ethernet and fabric path interfaces
- Changing switchport mode access or trunk to private VLAN or vice versa

### Licensing Requirements for Port Security

The following table shows the licensing requirements for this feature:

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>Port security requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS device images and is provided at no extra charge to you.</td>
</tr>
</tbody>
</table>

### Prerequisites for Port Security

### Guidelines and Limitations for Port Security

When configuring port security, follow these guidelines:

- Port security is supported on PVLAN ports.
- Port security does not support switched port analyzer (SPAN) destination ports.
- Port security does not depend upon other features.
- If any member link in a port-channel is in the pre-provisioned state, that is, the module is offline, then the port security feature cannot be disabled on the port-channel.
Guidelines and Limitations for Port Security on vPCs

In addition to the guidelines and limitations for port security, there are additional guidelines and limitations for port security on vPCs. When configuring port security on vPCs, follow these guidelines:

- You must enable port security globally on both vPC peers in a vPC domain.
- You must enable port security on the vPC interfaces of both vPC peers.
- You must configure a static secure MAC address on the primary vPC peer. This MAC address is synchronized with the secondary vPC peer. You can also configure a static secure MAC address on the secondary peer. This MAC address appears in the secondary vPC configuration, but does not take affect.
- All learned MAC addresses are synchronized between vPC peers.
- Both vPC peers can be configured with either the dynamic or sticky MAC address learning method. However, we recommend that both vPC peers be configured for the same method.
- Dynamic MAC addresses are dropped only after the age limit is reached on both vPC peers.
- You set the maximum number of secure MAC addresses on the primary vPC switch. The primary vPC switch does the count validation, even if a maximum number of secure MAC addresses is set on the secondary switch.
- You configure the violation action on the primary vPC. So, whenever a security violation is triggered, the security action defined on the primary vPC switch occurs.
- Port security is enabled on a vPC interface when the port security feature is enabled on both vPC peers and port security is enabled on both vPC interfaces of the vPC peers. You can use the `config sync` command to verify that the configuration is correct.
- While a switch undergoes an in-service software upgrade (ISSU), port security operations are stopped on its peer switch. The peer switch does not learn any new MAC addresses, and MAC moves occurring during this operation are ignored. When the ISSU is complete, the peer switch is notified and normal port security functionality resumes.
- ISSU to higher versions is supported; however ISSU to lower versions is not supported.

Default Settings for Port Security

This table lists the default settings for port security parameters.

Table 17: Default Port Security Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port security enablement globally</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port security enablement per interface</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC address learning method</td>
<td>Dynamic</td>
</tr>
</tbody>
</table>
Configuring Port Security

Enabling or Disabling Port Security Globally

You can enable or disable port security globally on a device. By default, port security is disabled globally.

When you disable port security, all port security configuration on the interface is ineffective. When you disable port security globally, all port security configuration is lost.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Example: | switch# configure terminal  
| | switch(config)# | |
| Step 2 | [no] feature port-security | Enables port security globally. The no option disables port security globally. |
| Example: | switch(config)# feature port-security | |
| Step 3 | show port-security | Displays the status of port security. |
| Example: | switch(config)# show port-security | |
| Step 4 | (Optional) copy running-config startup-config | Copies the running configuration to the startup configuration. |
| Example: | switch(config)# copy running-config startup-config | |

Enabling or Disabling Port Security on a Layer 2 Interface

You can enable or disable port security on a Layer 2 interface. By default, port security is disabled on all interfaces.
You can enable port-security on a port-channel in the following ways:

- Bundle member links into a port-channel by using the `channel-group` command and then enable port-security on the port-channel.

- Create port-channel and configure port security. Configure port security on member links and then bundle member links by using the `channel-group` command. In case of pre-provisioned member links, you can bundle them to the port-channel after the module is online.

**Before you begin**

You must have enabled port security globally.

If a Layer 2 Ethernet interface is a member of a port-channel interface, you cannot enable or disable port security on the Layer 2 Ethernet interface.

If any member port of a secure Layer 2 port-channel interface has port security enabled, you cannot disable port security for the port-channel interface unless you first remove all secure member ports from the port-channel interface.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters interface configuration mode for the Ethernet or port-channel interface that you want to configure with port security.</td>
</tr>
<tr>
<td>Enter one of the following commands:</td>
<td></td>
</tr>
<tr>
<td>• interface ethernet slot/port</td>
<td></td>
</tr>
<tr>
<td>• interface port-channel channel-number</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# interface ethernet 2/1</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-if)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the interface as a Layer 2 interface.</td>
</tr>
<tr>
<td>switchport</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config-if)# switchport</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables port security on the interface. The no option disables port security on the interface.</td>
</tr>
<tr>
<td>[no] switchport port-security</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config-if)# switchport port-security</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Displays the port security configuration.</td>
</tr>
<tr>
<td>show running-config port-security</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config-if)# show running-config port-security</code></td>
<td></td>
</tr>
</tbody>
</table>
### Enabling or Disabling Sticky MAC Address Learning

You can disable or enable sticky MAC address learning on an interface. If you disable sticky learning, the device returns to dynamic MAC address learning on the interface, which is the default learning method. By default, sticky MAC address learning is disabled.

**Before you begin**
You must have enabled port security globally.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Example: | switch# configure terminal  
switch(config)# | |
| **Step 2** | Enter one of the following commands:  
- interface ethernet slot/port  
- interface port-channel channel-number | Enters interface configuration mode for the interface that you want to configure with sticky MAC address learning. |
| Example: | switch(config)# interface ethernet 2/1  
switch(config-if)# | |
| **Step 3** | switchport | Configures the interface as a Layer 2 interface. |
| Example: | switch(config-if)# switchport | |
| **Step 4** | [no] switchport port-security mac-address sticky | Enables sticky MAC address learning on the interface. The no option disables sticky MAC address learning. |
| Example: | switch(config-if)# switchport port-security mac-address sticky | |
| **Step 5** | show running-config port-security | Displays the port security configuration. |
| Example: | switch(config-if)# show running-config port-security | |
### Adding a Static Secure MAC Address on an Interface

You can add a static secure MAC address on a Layer 2 interface.

**Note**

If the MAC address is a secure MAC address on any interface, you cannot add it as a static secure MAC address to another interface until you remove it from the interface on which it is already a secure MAC address.

By default, no static secure MAC addresses are configured on an interface.

**Before you begin**

You must have enabled port security globally.

Verify that the interface maximum has not been reached for secure MAC addresses. If needed, you can remove a secure MAC address or you can change the maximum number of addresses on the 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:switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter one of the following commands:</td>
<td>Enters interface configuration mode for the interface that you specify.</td>
</tr>
<tr>
<td></td>
<td>• interface ethernet slot/port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• interface port-channel channel-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:switch(config)# interface ethernet 2/1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)#</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>[no] switchport port-security mac-address address [vlan vlan-ID]</td>
<td>Configures a static MAC address for port security on the current interface. Use the <code>vlan</code> keyword if you want to specify the VLAN that traffic from the address is allowed on.</td>
</tr>
<tr>
<td></td>
<td>Example:switch(config-if)# switchport</td>
<td></td>
</tr>
<tr>
<td></td>
<td>port-security mac-address 0019.D2D0.00AE</td>
<td></td>
</tr>
</tbody>
</table>
### Removing a Static Secure MAC Address on an Interface

You can remove a static secure MAC address on a Layer 2 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>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter one of the following commands:</td>
<td>Enters interface configuration mode for the interface from which you want to remove a static secure MAC address.</td>
</tr>
<tr>
<td></td>
<td>• interface ethernet slot/port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• interface port-channel channel-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# interface ethernet 2/1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)#</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>no switchport port-security mac-address address</td>
<td>Removes the static secure MAC address from port security on the current interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)# no switchport</td>
<td></td>
</tr>
<tr>
<td></td>
<td>port-security mac-address 0019.D2D0.00AE</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>show running-config port-security</td>
<td>Displays the port security configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)# show running-config port-security</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config-if)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Removing a Sticky Secure MAC Address

You can remove a sticky secure MAC addresses, which requires that you temporarily disable sticky address learning on the interface that has the address that you want to remove.

**Before you begin**

You must have enabled port security globally.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Enter one of the following commands:</td>
<td>Enters interface configuration mode for the interface from which you want to remove a sticky secure MAC address.</td>
</tr>
<tr>
<td></td>
<td>• <code>interface ethernet slot/port</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>interface port-channel channel-number</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# interface ethernet 2/1</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-if)#</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>no switchport port-security mac-address sticky</code></td>
<td>Enables sticky MAC address learning on the interface, which converts any sticky secure MAC addresses on the interface to dynamic secure MAC addresses.</td>
</tr>
<tr>
<td></td>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-if)# no switchport port-security mac-address sticky</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>clear port-security dynamic address address</code></td>
<td>Removes the dynamic secure MAC address that you specify.</td>
</tr>
<tr>
<td></td>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-if)# clear port-security dynamic address 0019.D2D0.02GD</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><em>(Optional)</em> `show port-security address interface {ethernet slot/port</td>
<td>port-channel channel-number}*`</td>
</tr>
<tr>
<td></td>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# show port-security address</code></td>
<td></td>
</tr>
</tbody>
</table>
Removing a Dynamic Secure MAC Address

You can remove dynamically learned, secure MAC addresses.

Before you begin
You must have enabled port security globally.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal&lt;br&gt;<strong>Example:</strong> switch# configure terminal switch(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>clear port-security dynamic () [interface ethernet slot/port</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>show port-security address&lt;br&gt;<strong>Example:</strong> switch(config)# show port-security address</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>copy running-config startup-config&lt;br&gt;<strong>Example:</strong> switch(config-if)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

Enables sticky MAC address learning again on the interface.

Removes dynamically learned, secure MAC addresses, as specified.

Enters global configuration mode.

Removes all dynamically learned addresses on the interface that you specify.

If you use the interface keyword, you remove all dynamically learned addresses on the interface that you specify.

If you use the address keyword, you remove the single, dynamically learned address that you specify.

Use the vlan keyword if you want to further limit the command to removing an address or addresses on a particular VLAN.

Displays secure MAC addresses.

Copies the running configuration to the startup configuration.
Configuring a Maximum Number of MAC Addresses

You can configure the maximum number of MAC addresses that can be learned or statically configured on a Layer 2 interface. You can also configure a maximum number of MAC addresses per VLAN on a Layer 2 interface. The largest maximum number of addresses that you can configure on an interface is 1025 addresses. The system maximum number of address is 8192.

By default, an interface has a maximum of one secure MAC address. VLANs have no default maximum number of secure MAC addresses.

---

**Note**

When you specify a maximum number of addresses that is less than the number of addresses already learned or statically configured on the interface, the device rejects the command. To remove all addresses learned by the dynamic method, use the `shutdown` and `no shutdown` commands to restart the interface.

---

**Before you begin**

You must have enabled port security globally.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | **configure terminal**  
Example:  
```
switch# configure terminal
switch(config)#
``` | Enters global configuration mode. |
| Step 2 | Enter one of the following commands:  
- `interface ethernet slot/port`
- `interface port-channel channel-number`

Example:  
```
switch(config)# interface ethernet 2/1
switch(config-if)#
``` | Enters interface configuration mode, where `slot` is the interface that you want to configure with the maximum number of MAC addresses. |
| Step 3 | `[no] switchport port-security maximum number [vlan vlan-ID]`  
Example:  
```
switch(config-if)# switchport port-security maximum 425
``` | Configures the maximum number of MAC addresses that can be learned or statically configured for the current interface. The highest valid `number` is 1025. The `no` option resets the maximum number of MAC addresses to the default, which is 1. If you want to specify the VLAN that the maximum applies to, use the `vlan` keyword. |
| Step 4 | `show running-config port-security`  
Example:  
```
switch(config-if)# show running-config port-security
``` | Displays the port security configuration. |
### Configuring an Address Aging Type and Time

You can configure the MAC address aging type and the length of time that the device uses to determine when MAC addresses learned by the dynamic method have reached their age limit.

Absolute aging is the default aging type.

By default, the aging time is 0 minutes, which disables aging.

#### Before you begin

You must have enabled port security globally.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Enters interface configuration mode for the interface that you want to configure with the MAC aging type and time.</td>
</tr>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters interface configuration mode for the interface that you want to configure with the MAC aging type and time.</td>
</tr>
<tr>
<td><code>interface ethernet slot/port</code></td>
<td></td>
</tr>
<tr>
<td><code>interface port-channel channel-number</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Configures the type of aging that the device applies to dynamically learned MAC addresses. The no option resets the aging type to the default, which is absolute aging.</td>
</tr>
<tr>
<td><code>switch(config)# interface ethernet 2/1</code></td>
<td></td>
</tr>
<tr>
<td><code>switch(config-if)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the number of minutes that a dynamically learned MAC address must age before the device drops the address. The maximum valid minutes is 1440. The no option resets the aging time to the default, which is 0 minutes (no aging).</td>
</tr>
<tr>
<td><code>[no] switchport port-security aging time minutes</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config-if)# switchport port-security aging time 120</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>`[no] switchport port-security aging type {absolute</td>
<td>inactivity}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config-if)# switchport port-security aging type inactivity</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note**: F1 series modules do not support the inactivity aging type.
## Configuring a Security Violation Action

You can configure the action that the device takes if a security violation occurs. The violation action is configurable on each interface that you enable with port security.

The default security action is to shut down the port on which the security violation occurs.

### Before you begin

You must have enabled port security globally.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>switch# configure terminal switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 2** | Enter one of the following commands:  
  - `interface ethernet slot/port`  
  - `interface port-channel channel-number` | Enters interface configuration mode for the interface that you want to configure with a security violation action. |
| **Example:** | switch(config)# interface ethernet 2/1 switch(config-if)# | |
| **Step 3** | `[no] switchport port-security violation {protect | restrict | shutdown}` | Configures the security violation action for port security on the current interface. The `no` option resets the violation action to the default, which is to shut down the interface. |
| **Example:** | switch(config-if)# switchport port-security violation restrict | |
| **Step 4** | `show running-config port-security` | Displays the port security configuration. |
| **Example:** | | |
Verifying the Port Security Configuration

To display the port security configuration information, perform one of the following tasks. For detailed information about the fields in the output from this command, see the Cisco Nexus 7000 Series NX-OS Security Command Reference.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config port-security</td>
<td>Displays the port security configuration.</td>
</tr>
<tr>
<td>show port-security</td>
<td>Displays the port security status of the device.</td>
</tr>
<tr>
<td>show port-security interface</td>
<td>Displays the port security status of a specific interface.</td>
</tr>
<tr>
<td>show port-security address</td>
<td>Displays secure MAC addresses.</td>
</tr>
</tbody>
</table>

Displaying Secure MAC Addresses

Use the show port-security address command to display secure MAC addresses. For detailed information about the fields in the output from this command, see the

Configuration Example for Port Security

The following example shows a port security configuration for the Ethernet 2/1 interface with VLAN and interface maximums for secure addresses. In this example, the interface is a trunk port. Additionally, the violation action is set to Restrict.

```
feature port-security
interface Ethernet 2/1
switchport
switchport port-security
switchport port-security maximum 10
switchport port-security maximum 7 vlan 10
switchport port-security maximum 3 vlan 20
switchport port-security violation restrict
```
Configuration Example of Port Security in a vPC Domain

The following example shows how to enable and configure port security on vPC peers in a vPC domain. The first switch is the primary vPC peer and the second switch is the secondary vPC peer. It is assumed that domain 103 has already been created.

```
primary_switch(config)# feature port-security
primary_switch(config-if)# int e1/1
primary_switch(config-if)# switchport port-security
primary_switch(config-if)# switchport port-security max 1025
primary_switch(config-if)# switchport port-security violation restrict
primary_switch(config-if)# switchport port-security aging time 4
primary_switch(config-if)# switchport port-security aging type absolute
primary_switch(config-if)# switchport port-security mac sticky
primary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
primary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
primary_switch(config-if)# copy running-config startup-config

secondary_switch(config)# int e103/1/1
secondary_switch(config-if)# switchport port-security
secondary_switch(config-if)# copy running-config startup-config
```

Additional References for Port Security

Related Documents

Standards

<table>
<thead>
<tr>
<th>Standards</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

Cisco NX-OS provides read-only SNMP support for port security.

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-PORT-SECURITY-MIB</td>
<td>To locate and download MIBs, go to the following URL: <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>

Note

Traps are supported for notification of secure MAC address violations.
CHAPTER 11

Configuring DHCP Snooping

This chapter contains the following sections:

- Information About DHCP Snooping, on page 201
- Information About the DHCP Relay Agent, on page 206
- Information about the DHCPv6 Relay Agent, on page 207
- Information About the Lightweight DHCPv6 Relay Agent, on page 207
- Guidelines and Limitations for DHCP Snooping, on page 208
- Default Settings for DHCP Snooping, on page 208
- Configuring DHCP Snooping, on page 209
- Configuring the DHCPv6 Relay Agent, on page 219
- Configuring Lightweight DHCPv6 Relay Agent, on page 222
- Verifying the DHCP Snooping Configuration, on page 224
- Displaying DHCP Bindings, on page 224
- Displaying and Clearing LDRA Information, on page 225
- Clearing the DHCP Snooping Binding Database, on page 225
- Clearing DHCP Relay Statistics, on page 226
- Clearing DHCPv6 Relay Statistics, on page 226
- Monitoring DHCP, on page 226
- Configuration Examples for DHCP Snooping, on page 226
- Configuration Examples for LDRA, on page 227

Information About DHCP Snooping

DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers. DHCP snooping performs the following activities:

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
- Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
- Uses the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.
Feature Enabled and Globally Enabled

When you are configuring DHCP snooping, it is important that you understand the difference between enabling the DHCP snooping feature and globally enabling DHCP snooping.

**Feature Enablement**

The DHCP snooping feature is disabled by default. When the DHCP snooping feature is disabled, you cannot configure it or any of the features that depend on DHCP snooping. The commands to configure DHCP snooping and its dependent features are unavailable when DHCP snooping is disabled.

When you enable the DHCP snooping feature, the switch begins building and maintaining the DHCP snooping binding database. Features dependent on the DHCP snooping binding database can now make use of it and can therefore also be configured.

Enabling the DHCP snooping feature does not globally enable it. You must separately enable DHCP snooping globally.

Disabling the DHCP snooping feature removes all DHCP snooping configuration from the switch. If you want to disable DHCP snooping and preserve the configuration, globally disable DHCP snooping but do not disable the DHCP snooping feature.

**Global Enablement**

After DHCP snooping is enabled, DHCP snooping is globally disabled by default. Global enablement is a second level of enablement that allows you to have separate control of whether the switch is actively performing DHCP snooping that is independent from enabling the DHCP snooping binding database.

When you globally enable DHCP snooping, on each untrusted interface of VLANs that have DHCP snooping enabled, the switch begins validating DHCP messages that are received and used the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

When you globally disable DHCP snooping, the switch stops validating DHCP messages and validating subsequent requests from untrusted hosts. It also removes the DHCP snooping binding database. Globally disabling DHCP snooping does not remove any DHCP snooping configuration or the configuration of other features that are dependent upon the DHCP snooping feature.

**Trusted and Untrusted Sources**

You can configure whether DHCP snooping trusts traffic sources. An untrusted source might initiate traffic attacks or other hostile actions. To prevent such attacks, DHCP snooping filters messages from untrusted sources.

In an enterprise network, a trusted source is a switch that is under your administrative control. These switches include the switches, routers, and servers in the network. Any switch beyond the firewall or outside the network is an untrusted source. Generally, host ports are treated as untrusted sources.

In a service provider environment, any switch that is not in the service provider network is an untrusted source (such as a customer switch). Host ports are untrusted sources.

In a Cisco Nexus device, you indicate that a source is trusted by configuring the trust state of its connecting interface.

The default trust state of all interfaces is untrusted. You must configure DHCP server interfaces as trusted. You can also configure other interfaces as trusted if they connect to switches (such as switches or routers) inside your network. You usually do not configure host port interfaces as trusted.
For DHCP snooping to function properly, you must connect all DHCP servers to the switch through trusted interfaces.

---

**DHCP Snooping Binding Database**

Using information extracted from intercepted DHCP messages, DHCP snooping dynamically builds and maintains a database. The database contains an entry for each untrusted host with a leased IP address if the host is associated with a VLAN that has DHCP snooping enabled. The database does not contain entries for hosts that are connected through trusted interfaces.

---

**Note**
The DHCP snooping binding database is also referred to as the DHCP snooping binding table.

---

DHCP snooping updates the database when the switch receives specific DHCP messages. For example, the feature adds an entry to the database when the switch receives a DHCPACK message from the server. The feature removes the entry in the database when the IP address lease expires or the switch receives a DHCPRELEASE message from the host.

Each entry in the DHCP snooping binding database includes the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host.

You can remove entries from the binding database by using the `clear ip dhcp snooping binding` command.

---

**DHCP Snooping Option 82 Data Insertion**

DHCP can centrally manage the IP address assignments for a large number of subscribers. When you enable Option 82, the device identifies a subscriber device that connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can connect to the same port on the access device and are uniquely identified.

When you enable Option 82 on the Cisco NX-OS device, the following sequence of events occurs:

1. The host (DHCP client) generates a DHCP request and broadcasts it on the network.

2. When the Cisco NX-OS device receives the DHCP request, it adds the Option 82 information in the packet. The Option 82 information contains the device MAC address (the remote ID suboption) and the port identifier, vlan-mod-port, from which the packet is received (the circuit ID suboption). For hosts behind the port channel, the circuit ID is filled with the if_index of the port channel.

3. The device forwards the DHCP request that includes the Option 82 field to the DHCP server.

4. 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. The DHCP server echoes the Option 82 field in the DHCP reply.

5. The DHCP server sends the reply to the Cisco NX-OS device. The Cisco NX-OS device verifies that it originally inserted the Option 82 data by inspecting the remote ID and possibly the circuit ID fields.
Cisco NX-OS device removes the Option 82 field and forwards the packet to the interface that connects to the DHCP client that sent the DHCP request.

If the previously described sequence of events occurs, the following values do not change:

- 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 circuit ID type

**Figure 13: Suboption Packet Formats**

This figure shows the packet formats for the remote ID suboption and the circuit ID suboption. The Cisco NX-OS device uses the packet formats when you globally enable DHCP snooping and when you enable Option 82 data insertion and removal. For the circuit ID suboption, the module field is the slot number of the module.

**Circuit ID Suboption Frame Format**

```
<table>
<thead>
<tr>
<th>Suboption type</th>
<th>Circuit ID type</th>
<th>VLAN</th>
<th>Module</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>Length</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>MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>Length</td>
<td>1 byte</td>
</tr>
</tbody>
</table>
```
DHCP Snooping in a vPC Environment

A virtual port channel (vPC) allows two Cisco NX-OS switches to appear as a single logical port channel to a third switch. The third switch can be a switch, server, or any other networking switch that supports port channels.

In a typical vPC environment, DHCP requests can reach one vPC peer switch and the responses can reach the other vPC peer switch, resulting in a partial DHCP (IP-MAC) binding entry in one switch and no binding entry in the other switch. This issue is addressed by using Cisco Fabric Service over Ethernet (CFSoE) distribution to ensure that all DHCP packets (requests and responses) appear on both switches, which helps in creating and maintaining the same binding entry on both switches for all clients behind the vPC link.

CFSoE distribution also allows only one switch to forward the DHCP requests and responses on the vPC link. In non-vPC environments, both switches forward the DHCP packets.

Synchronizing DHCP Snooping Binding Entries

The dynamic DHCP binding entries should be in sync in the following scenarios:

- When the remote vPC is online, all the binding entries for that vPC link should be in sync with the peer.
- When DHCP snooping is enabled on the peer switch, the dynamic binding entries for all vPC links that are up remotely should be in sync with the peer.

Packet Validation

The switch validates DHCP packets received on the untrusted interfaces of VLANs that have DHCP snooping enabled. The switch forwards the DHCP packet unless any of the following conditions occur (in which case, the packet is dropped):

- The switch receives a DHCP response packet (such as a DHCPACK, DHCPNAK, or DHCPOFFER packet) on an untrusted interface.
- The switch receives a packet on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match. This check is performed only if the DHCP snooping MAC address verification option is turned on.
- The switch receives a DHCPRELEASE or DHCPDECLINE message from an untrusted host with an entry in the DHCP snooping binding table, and the interface information in the binding table does not match the interface on which the message was received.

In addition, you can enable strict validation of DHCP packets, which checks the options field of DHCP packets, including the “magic cookie” value in the first four bytes of the options field. By default, strict validation is disabled. When you enable it, by using the `ip dhcp packet strict-validation` command, if DHCP snooping processes a packet that has an invalid options field, it drops the packet.
Information About the DHCP Relay Agent

DHCP Relay Agent

You can configure the device to run a DHCP relay agent, which forwards DHCP packets between clients and servers. This feature is useful when clients and servers are not on the same physical subnet. Relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The relay agent sets the gateway address (giaddr field of the DHCP packet) and, if configured, adds the relay agent information option (Option 82) in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing Option 82.

After you enable Option 82, the device uses the binary ifindex format by default. If needed, you can change the Option 82 setting to use an encoded string format instead.

Note

When the device relays a DHCP request that already includes Option 82 information, the device forwards the request with the original Option 82 information without altering it.

VRF Support for the DHCP Relay Agent

You can configure the DHCP relay agent to forward DHCP broadcast messages from clients in a virtual routing and forwarding (VRF) instance to DHCP servers in a different VRF. By using a single DHCP server to provide DHCP support to clients in multiple VRFs, you can conserve IP addresses by using a single IP address pool rather than one for each VRF.

Enabling VRF support for the DHCP relay agent requires that you enable Option 82 for the DHCP relay agent. If a DHCP request arrives on an interface that you have configured with a DHCP relay address and VRF information, and the address of the DHCP server belongs to a network on an interface that is a member of a different VRF, the device inserts Option 82 information in the request and forwards it to the DHCP server in the server VRF. The Option 82 information includes the following:

VPN identifier

Name of the VRF that the interface that receives the DHCP request is a member of.

Link selection

Subnet address of the interface that receives the DHCP request.

Server identifier override

IP address of the interface that receives the DHCP request.

Note

The DHCP server must support the VPN identifier, link selection, and server identifier override options.

When the device receives the DHCP response message, it strips off the Option 82 information and forwards the response to the DHCP client in the client VRF.
DHCP Relay Binding Database

A relay binding is an entity that associates a DHCP or BOOTP client with a relay agent address and its subnet. Each relay binding stores the client MAC address, active relay agent address, active relay agent address mask, logical and physical interfaces to which the client is connected, giaddr retry count, and total retry count. The giaddr retry count is the number of request packets transmitted with that relay agent address, and the total retry count is the total number of request packets transmitted by the relay agent. One relay binding entry is maintained for each DHCP or BOOTP client.

Information about the DHCPv6 Relay Agent

DHCPv6 Relay Agent

You can configure the device to run a DHCPv6 relay agent, which forwards DHCPv6 packets between clients and servers. This feature is useful when clients and servers are not on the same physical subnet. Relay agents receive DHCPv6 messages and then generate a new DHCPv6 message to send out on another interface. The relay agent sets the gateway address (giaddr field of the DHCPv6 packet) and forwards it to the DHCPv6 server.

VRF Support for the DHCPv6 Relay Agent

You can configure the DHCPv6 relay agent to forward DHCPv6 broadcast messages from clients in a virtual routing and forwarding (VRF) instance to DHCPv6 servers in a different VRF. By using a single DHCPv6 server to provide DHCPv6 support to clients in multiple VRFs, you can conserve IP addresses by using a single IP address pool rather than one for each VRF.

Information About the Lightweight DHCPv6 Relay Agent

Lightweight DHCPv6 Relay Agent

A variety of different link-layer network topologies exist for the aggregation of IPv6 nodes into one or more routers. In Layer 2 aggregation networks (IEEE 802.1D bridging or similar) that have many nodes on a single link, a DHCP Version 6 (DHCPv6) server or DHCP relay agent normally does not recognize how a DHCP client is attached to a network. From Cisco NX-OS Release , you can configure the interface of a device to run Lightweight DHCPv6 Relay Agent (LDRA), which forwards DHCPv6 messages between clients and servers.

The LDRA feature is used to insert relay agent options in DHCPv6 message exchanges primarily to identify client-facing interfaces. LDRA resides on the same IPv6 link as the client and a DHCPv6 relay agent or server.

LDRA for VLANs and Interfaces

You can configure LDRA on VLANs and interfaces. LDRA is not enabled by default. To enable LDRA, it should be enabled globally and at the interface level. You should configure the interfaces as client-facing trusted, client-facing untrusted, or server-facing. All client-facing interfaces must be configured as trusted or...
untrusted. By default, all the client-facing interfaces in LDRA are configured as untrusted. When a client-facing interface is deemed untrusted, LDRA will discard messages of type RELAY-FORWARD, which are received from the client-facing interface.

The LDRA configuration on a VLAN should be configured as client-facing trusted or client-facing untrusted. When you configure LDRA functionality on a VLAN, the functionality is configured on all the ports or interfaces within the VLAN. However, if you configure an interface in a VLAN as client-facing untrusted, and configure the VLAN as client-facing trusted, the configuration of an interface takes precedence over the configuration of a VLAN. At least one interface in a VLAN should be configured as server-facing interface.

Guidelines and Limitations for Lightweight DHCPv6 Relay Agent

- Access nodes implementing LDRA do not support IPv6 control or routing.
- An interface or port cannot be configured as both client facing and server facing at the same time.
- To support virtual port channel, LDRA configuration should be symmetric on the vPC peers.
- LDRA supports Cisco Fabricpath.

Guidelines and Limitations for DHCP Snooping

Consider the following guidelines and limitations when configuring DHCP snooping:

- The DHCP snooping database can store 2000 bindings.
- DHCP snooping is not active until you enable the feature, enable DHCP snooping globally, and enable DHCP snooping on at least one VLAN.
- Before globally enabling DHCP snooping on the switch, make sure that the switches that act as the DHCP server and the DHCP relay agent are configured and enabled.
- If a VLAN ACL (VACL) is configured on a VLAN that you are configuring with DHCP snooping, ensure that the VACL permits DHCP traffic between DHCP servers and DHCP hosts.
- DHCP snooping does not work with DHCP relay configured on the same nexus device.
- When you configure DHCPv6 server addresses on an interface, a destination interface cannot be used with global IPv6 addresses.

Default Settings for DHCP Snooping

This table lists the default settings for DHCP snooping parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP snooping feature</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping globally enabled</td>
<td>No</td>
</tr>
</tbody>
</table>
Configuring DHCP Snooping

Minimum DHCP Snooping Configuration

1. Enable the DHCP snooping feature.
2.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Enable the DHCP snooping feature.</td>
<td>When the DHCP snooping feature is disabled, you cannot configure DHCP snooping. For details, see Enabling or Disabling the DHCP Snooping Feature, on page 209.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Enable DHCP snooping globally.</td>
<td>For details, see Enabling or Disabling DHCP Snooping Globally, on page 210.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Enable DHCP snooping on at least one VLAN.</td>
<td>By default, DHCP snooping is disabled on all VLANs. For details, see Enabling or Disabling DHCP Snooping on a VLAN, on page 211.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Ensure that the DHCP server is connected to the switch using a trusted interface.</td>
<td>For details, see Configuring an Interface as Trusted or Untrusted, on page 213.</td>
</tr>
</tbody>
</table>

Enabling or Disabling the DHCP Snooping Feature

You can enable or disable the DHCP snooping feature on the switch. By default, DHCP snooping is disabled.
Before you begin

If you disable the DHCP snooping feature, all DHCP snooping configuration is lost. If you want to turn off DHCP snooping and preserve the DHCP snooping configuration, disable DHCP globally.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> [no] feature dhcp</td>
<td>Enables the DHCP snooping feature. The no option disables the DHCP snooping feature and erases all DHCP snooping configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# feature dhcp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) show running-config dhcp</td>
<td>Shows the DHCP snooping configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# show running-config dhcp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Enabling or Disabling DHCP Snooping Globally

You can enable or disable the DHCP snooping globally on the switch. Globally disabling DHCP snooping stops the switch from performing any DHCP snooping but preserves DHCP snooping configuration.

Before you begin

Ensure that you have enabled the DHCP snooping feature. By default, DHCP snooping is globally disabled.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> [no] ip dhcp snooping</td>
<td>Enables DHCP snooping globally. The no option disables DHCP snooping.</td>
</tr>
<tr>
<td><strong>Example:</strong> switch(config)# ip dhcp snooping</td>
<td></td>
</tr>
</tbody>
</table>
### Enabling or Disabling DHCP Snooping on a VLAN

You can enable or disable DHCP snooping on one or more VLANs.

**Before you begin**

By default, DHCP snooping is disabled on all VLANs.

Ensure that DHCP snooping is enabled.

---

**Note**

If a VACL is configured on a VLAN that you are configuring with DHCP snooping, ensure that the VACL permits DHCP traffic between DHCP servers and DHCP hosts.

---

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>[no] ip dhcp snooping vlan vlan-list</td>
<td>Enables DHCP snooping on the VLANs specified by <code>vlan-list</code>. The no option disables DHCP snooping on the VLANs specified.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# ip dhcp snooping vlan 100,200,250-252</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>(Optional) show running-config dhcp</td>
<td>Shows the DHCP snooping configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# show running-config dhcp</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>(Optional) copy running-config startup-config</td>
<td>Copies the running configuration to the startup configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Enabling or Disabling Option 82 Data Insertion and Removal

You can enable or disable the insertion and removal of Option 82 information for DHCP packets forwarded without the use of the DHCP relay agent.

Before you begin

By default, the switch does not include Option 82 information in DHCP packets.

Ensure that DHCP snooping is enabled.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| `switch# configure terminal`  
  `switch(config)#` | |
| `[no] ip dhcp snooping information option` | Enables the insertion and removal of Option 82 information from DHCP packets. The `no` option disables the insertion and removal of Option 82 information. |
| `switch(config)# ip dhcp snooping information option` | |
| `show running-config dhcp` | Shows the DHCP snooping configuration. |
| `switch(config)# show running-config dhcp` | |
| `(Optional) copy running-config startup-config` | Copies the running configuration to the startup configuration. |
| `switch(config)# copy running-config startup-config` | |

Enabling or Disabling Strict DHCP Packet Validation

You can enable or disable the strict validation of DHCP packets by the DHCP snooping feature. By default, strict validation of DHCP packets is disabled.
## Configuring an Interface as Trusted or Untrusted

You can configure whether an interface is a trusted or untrusted source of DHCP messages. You can configure DHCP trust on the following types of interfaces:

- Layer 2 Ethernet interfaces
- Layer 2 port-channel interfaces

### Before you begin

By default, all interfaces are untrusted.

Ensure that DHCP snooping is enabled.

### 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>
</tbody>
</table>
| Example: | switch# configure terminal  
| | switch(config)# |

Enters global configuration mode.

| **Step 2** | [no] ip dhcp packet strict-validation |
| Example: | switch(config)# ip dhcp packet  
| | strict-validation |

Enables the strict validation of DHCP packets by the DHCP snooping feature. The **no** option disables strict DHCP packet validation.

| **Step 3** | (Optional) show running-config dhcp |
| Example: | switch(config)# show running-config dhcp |

Shows the DHCP snooping configuration.

| **Step 4** | (Optional) copy running-config startup-config |
| Example: | switch(config)# copy running-config  
| | startup-config |

Copies the running configuration to the startup configuration.
### Configuring DHCP Snooping

#### Enabling or Disabling the DHCP Relay Agent

You can enable or disable the DHCP relay agent. By default, the DHCP relay agent is enabled.

**Before you begin**

Ensure that the DHCP feature is enabled.

**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>config t</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** | switch# config t  
switch(config)# | |
| **Step 2** | `[no] ip dhcp relay` | Enables the DHCP relay agent. The `no` option disables the relay agent. |
| **Example:** | switch(config)# ip dhcp relay | |
| **Step 3** | `(Optional) show ip dhcp relay` | Displays the DHCP relay configuration. |
| **Example:** | switch(config)# show ip dhcp relay | |

#### Enabling or Disabling the DHCP Relay Agent

You can enable or disable the DHCP relay agent. By default, the DHCP relay agent is enabled.

**Before you begin**

Ensure that the DHCP feature is enabled.

**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>config t</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** | switch# config t  
switch(config)# | |
| **Step 2** | `[no] ip dhcp relay` | Enables the DHCP relay agent. The `no` option disables the relay agent. |
| **Example:** | switch(config)# ip dhcp relay | |
| **Step 3** | `(Optional) show ip dhcp relay` | Displays the DHCP relay configuration. |
| **Example:** | switch(config)# show ip dhcp relay | |

---

### Enabling or Disabling the DHCP Relay Agent

You can enable or disable the DHCP relay agent. By default, the DHCP relay agent is enabled.

**Before you begin**

Ensure that the DHCP feature is enabled.

**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>config t</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** | switch# config t  
switch(config)# | |
| **Step 2** | `[no] ip dhcp relay` | Enables the DHCP relay agent. The `no` option disables the relay agent. |
| **Example:** | switch(config)# ip dhcp relay | |
| **Step 3** | `(Optional) show ip dhcp relay` | Displays the DHCP relay configuration. |
| **Example:** | switch(config)# show ip dhcp relay | |
Enabling or Disabling Option 82 for the DHCP Relay Agent

You can enable or disable the device to insert and remove Option 82 information on DHCP packets forwarded by the relay agent.

By default, the DHCP relay agent does not include Option 82 information in DHCP packets.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>[no] ip dhcp relay</td>
<td>Enables the DHCP relay feature. The <strong>no</strong> option disables this behavior.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# ip dhcp relay</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>[no] ip dhcp relay information option</td>
<td>Enables the DHCP relay agent to insert and remove Option 82 information on the packets that it forwards. The Option 82 information is in binary ifindex format by default. The <strong>no</strong> option disables this behavior.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# ip dhcp relay information option</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>(Optional) show ip dhcp relay</td>
<td>Displays the DHCP relay configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# show ip dhcp relay</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>(Optional) show running-config dhcp</td>
<td>Displays the DHCP configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch(config)# show running-config dhcp</td>
<td></td>
</tr>
</tbody>
</table>
Enabling or Disabling VRF Support for the DHCP Relay Agent

You can configure the device to support the relaying of DHCP requests that arrive on an interface in one VRF to a DHCP server in a different VRF instance.

Before you begin
You must enable Option 82 for the DHCP relay agent.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>config t</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch# config t</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)#</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>[no] ip dhcp relay information option vpn</code></td>
<td>Enables VRF support for the DHCP relay agent. The no option disables this behavior.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# ip dhcp relay information option vpn</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>[no] ip dhcp relay sub-option type cisco</code></td>
<td>Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID suboptions. The no option causes DHCP to use RFC numbers 5, 11, and 151 for the link selection, server ID override, and VRF name/VPN ID suboptions.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# ip dhcp relay sub-option type cisco</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>(Optional) <code>show ip dhcp relay</code></td>
<td>Displays the DHCP relay configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# show ip dhcp relay</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>(Optional) <code>show running-config dhcp</code></td>
<td>Displays the DHCP configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# show running-config dhcp</code></td>
<td></td>
</tr>
</tbody>
</table>
Enabling or Disabling Subnet Broadcast Support for the DHCP Relay Agent on a Layer 3 Interface

You can configure the device to support the relaying of DHCP packets from clients to a subnet broadcast IP address. When this feature is enabled, the VLAN ACLs (VACLs) accept IP broadcast packets and all subnet broadcast (primary subnet broadcast as well as secondary subnet broadcast) packets.

**Before you begin**
- Ensure that the DHCP feature is enabled.
- Ensure that the DHCP relay agent is enabled.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> config t</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: switch# config t switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface slot/port</td>
<td>Enters interface configuration mode, where slot/port is the interface for which you want to enable or disable subnet broadcast support for the DHCP relay agent.</td>
</tr>
<tr>
<td>Example: switch(config)# interface ethernet 2/2 switch(config-if)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> [no] ip dhcp relay subnet-broadcast</td>
<td>Enables subnet broadcast support for the DHCP relay agent. The no option disables this behavior.</td>
</tr>
<tr>
<td>Example: switch(config-if)# ip dhcp relay subnet-broadcast</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td>Example: switch(config-if)# exit switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td>Example: switch(config)# exit switch#</td>
<td></td>
</tr>
</tbody>
</table>
Creating a DHCP Static Binding

You can create a static DHCP source binding to a Layer 2 interface.

Before you begin

Ensure that you have enabled the DHCP snooping feature.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ip source binding <strong>IP-address</strong> MAC-address</td>
<td>Binds the static source address to the Layer 2 Ethernet interface.</td>
</tr>
<tr>
<td>vlan <strong>vlan-id</strong> {interface ethernet slot/port</td>
<td>Example: switch(config)# ip source binding</td>
</tr>
<tr>
<td>port-channel channel-no}</td>
<td>10.5.22.7 001f.28bd.0013 vlan 100</td>
</tr>
<tr>
<td>interface ethernet 2/3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) show ip dhcp snooping binding</td>
<td>Shows the DHCP snooping static and dynamic bindings.</td>
</tr>
<tr>
<td>Example: switch(config)# ip dhcp</td>
<td></td>
</tr>
<tr>
<td>snooping binding</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) show ip dhcp snooping binding</td>
<td>Shows the DHCP snooping dynamic bindings.</td>
</tr>
<tr>
<td>dynamic</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Configuring DHCP Snooping

Conﬁguring the DHCPv6 Relay Agent

Enabling or Disabling the DHCPv6 Relay Agent

**Before you begin**

Ensure that the DHCP feature is enabled.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  config terminal  |
  Example:
  switch# configure terminal
  switch(config)# |
| Enters global conﬁguration mode. |
| **Step 2**
  [no] ipv6 dhcp relay  |
  Example:
  switch(config)# ipv6 dhcp relay |
| Enables the DHCPv6 relay agent. The no option disables the relay agent. |
| **Step 3**
  (Optional) show ipv6 dhcp relay [interface interface]  |
  Example:
  switch(config)# show ipv6 dhcp relay |
| Displays the DHCPv6 relay conﬁguration. |
Enabling or Disabling VRF Support for the DHCPv6 Relay Agent

You can configure the device to support the relaying of DHCPv6 requests that arrive on an interface in one VRF to a DHCPv6 server in a different VRF.

Before you begin
Ensure that the DHCP feature is enabled.
Ensure that the DHCPv6 relay agent is enabled.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 2 [no] ipv6 dhcp relay option vpn</td>
<td>Enables VRF support for the DHCPv6 relay agent. The no option disables this behavior.</td>
</tr>
<tr>
<td>Example: switch(config)# ipv6 dhcp relay option vpn</td>
<td></td>
</tr>
<tr>
<td>Step 3 [no] ipv6 dhcp relay option type cisco</td>
<td>Causes the DHCPv6 relay agent to insert virtual subnet selection (VSS) details as part of the vendor-specific option. The no option causes the DHCPv6 relay agent to insert VSS details as part of the VSS option (68), which is defined in RFC-6607. This command is useful when you want to use DHCPv6 servers that do not support RFC-6607 but allocate IPv6 addresses based on the client VRF name.</td>
</tr>
<tr>
<td>Example: switch(config)# ipv6 dhcp relay option type cisco</td>
<td></td>
</tr>
<tr>
<td>Step 4 (Optional) show ipv6 dhcp relay [interface interface]</td>
<td>Displays the DHCPv6 relay configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring DHCPv6 Relay Source Interface

You can configure the source interface for the DHCPv6 relay agent. By default, the DHCPv6 relay agent uses the relay agent address as the source address of the outgoing packet. Configuring the source interface enables you to use a more stable address (such as the loopback interface address) as the source address of relayed messages.

#### Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the DHCPv6 relay agent is enabled.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>[no] ipv6 dhcp relay source-interface interface</td>
<td>Configures the source interface for the DHCPv6 relay agent.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# ipv6 dhcp relay source-interface loopback 2</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The DHCPv6 relay source interface can be configured globally, per interface, or both. When both the global and interface levels are configured, the interface-level configuration overrides the global configuration.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional) show ipv6 dhcp relay [interface interface]</td>
<td>Displays the DHCPv6 relay configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>switch(config)# show ipv6 dhcp relay</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring Lightweight DHCPv6 Relay Agent

### Configuring Lightweight DHCPv6 Relay Agent for an Interface

Perform this task to configure Lightweight DHCPv6 Relay Agent (LDRA) for 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><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
<td>Enables the LDRA functionality globally.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>interface slot/port</code></td>
<td>Specifies an interface type and number, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config)# interface ethernet 0/0</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>switchport</code></td>
<td>Switches an interface that is in Layer 3 mode to Layer 2 mode for Layer 2 configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>switch(config-if)# switchport</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>`[no] ipv6 dhcp-ldra {client-facing-trusted</td>
<td>client-facing-untrusted</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

### Configuring DHCP Snooping

---
### Configuring Lightweight DHCPv6 Relay Agent for a VLAN

Perform this task to configure Lightweight DHCPv6 Relay Agent (LDRA) for a VLAN.

**Before you begin**

Ensure that the VLAN is not assigned an IP address.

**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>switch# configure terminal</td>
<td>Example:</td>
</tr>
<tr>
<td>Step 2</td>
<td>Example:</td>
<td>Enables the LDRA functionality globally.</td>
</tr>
<tr>
<td>Step 3</td>
<td>[no] ipv6 dhcp-ldra attach–policy vlan vlan-id [client-facing-trusted</td>
<td>Enables LDRA functionality on the specified VLAN. The no option disables the LDRA functionality.</td>
</tr>
<tr>
<td></td>
<td>client-facing-untrusted]</td>
<td>Example:</td>
</tr>
</tbody>
</table>
Verifying the DHCP Snooping Configuration

To display DHCP snooping configuration information, perform one of the following tasks. For detailed information about the fields in the output from these commands, see the System Management Configuration Guide for your Cisco Nexus device.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config dhcp</td>
<td>Displays the DHCP snooping configuration.</td>
</tr>
<tr>
<td>show ip dhcp relay</td>
<td>Displays the DHCP relay configuration.</td>
</tr>
<tr>
<td>show ipv6 dhcp relay [interface interface]</td>
<td>Displays the DHCPv6 relay global or interface-level configuration.</td>
</tr>
<tr>
<td>show ip dhcp snooping</td>
<td>Displays general information about DHCP snooping.</td>
</tr>
</tbody>
</table>

Displaying DHCP Bindings

Use the show ip dhcp snooping binding command to display the DHCP static and dynamic binding table. Use the show ip dhcp snooping binding dynamic to display the DHCP dynamic binding table.

For detailed information about the fields in the output from this command, see the System Management Configuration Guide for your Cisco Nexus device.

This example shows how to create a static DHCP binding and then verify the binding using the show ip dhcp snooping binding command.

```
switch# configuration terminal
switch(config)# ip source binding 10.20.30.40 0000.1111.2222 vlan 400 interface port-channel 500
switch(config)# show ip dhcp snooping binding
MacAddress     IpAddress    LeaseSec Type   VLAN     Interface
-------------- ----------- ------- ----- ------- ------------
00:00:11:11:22:22 10.20.30.40 infinite static 400 port-channel1500
```
### Displaying and Clearing LDRA Information

To clear the DHCPv6 LDRA-specific statistics, use the `clear ipv6 dhcp-ldra statistics` command.

### Clearing the DHCP Snooping Binding Database

You can remove entries from the DHCP snooping binding database, including a single entry, all entries associated with an interface, or all entries in the database.

**Before you begin**

Ensure that DHCP snooping is enabled.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | (Optional) `clear ip dhcp snooping binding`  
**Example:**  
`switch# clear ip dhcp snooping binding` | Clears all entries from the DHCP snooping binding database. |
| 2    | (Optional) `clear ip dhcp snooping binding interface ethernet slot/port[,subinterface-number]`  
**Example:**  
`switch# clear ip dhcp snooping binding interface ethernet 1/4` | Clears entries associated with a specific Ethernet interface from the DHCP snooping binding database. |
| 3    | (Optional) `clear ip dhcp snooping binding interface port-channel channel-number[,subchannel-number]`  
**Example:**  
`switch# clear ip dhcp snooping binding interface port-channel 72` | Clears entries associated with a specific port-channel interface from the DHCP snooping binding database. |
| 4    | (Optional) `clear ip dhcp snooping binding vlan vlan-id mac mac-address ip ip-address interface {ethernet slot/port[,subinterface-number] | port-channel channel-number[,subchannel-number] }`  
**Example:**  
`switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface ethernet 2/11` | Clears a single, specific entry from the DHCP snooping binding database. |
| 5    | (Optional) `show ip dhcp snooping binding`  
**Example:** | Displays the DHCP snooping binding database. |
### Clearing DHCP Relay Statistics

Use the `clear ip dhcp relay statistics` command to clear the global DHCP relay statistics.

Use the `clear ip dhcp relay statistics interface interface` command to clear the DHCP relay statistics for a particular interface.

Use the `clear ip dhcp relay statistics interface interface serverip ip-address [use-vrf vrf-name]` command to clear the DHCP relay statistics at the server level for a particular interface.

### Clearing DHCPv6 Relay Statistics

Use the `clear ipv6 dhcp relay statistics` command to clear the global DHCPv6 relay statistics.

Use the `clear ipv6 dhcp relay statistics interface interface` command to clear the DHCPv6 relay statistics for a particular interface.

Use the `clear ipv6 dhcp relay statistics interface interface server-ip ip-address [use-vrf vrf-name]` command to clear the DHCPv6 relay statistics at the server level for a particular interface.

### Monitoring DHCP

Use the `show ip dhcp snooping statistics` command to monitor DHCP snooping.

Use the `show ip dhcp relay statistics [interface interface [serverip ip-address [use-vrf vrf-name]]]` command to monitor DHCP relay statistics at the global, server, or interface level.

Use the (Optional) `show ip dhcp snooping statistics vlan [vlan-id] interface [ethernet|port-channel][id]` command to know the exact statistics about snooping statistics per interface under a vlan.

### Configuration Examples for DHCP Snooping

The following example shows how to enable DHCP snooping on two VLANs, with Option 82 support enabled and Ethernet interface 2/5 trusted because the DHCP server is connected to that interface:

```bash
feature dhcp
ip dhcp snooping
ip dhcp snooping info option

interface Ethernet 2/5
  ip dhcp snooping trust
  ip dhcp snooping vlan 1
  ip dhcp snooping vlan 50
```
Configuration Examples for LDRA

Configuring LDRA for an Interface
The following example shows how to enable LDRA and configure interface Ethernet 1/1 as client-facing and trusted:

Configuring LDRA for a VLAN
The following example shows how to enable LDRA and configure VLAN with VLAN ID 25 as client-facing and trusted:
Configuring Control Plane Policing

This chapter contains the following sections:

- Information About CoPP, on page 229
- Control Plane Protection, on page 230
- CoPP Policy Templates, on page 234
- CoPP and the Management Interface, on page 239
- Licensing Requirements for CoPP, on page 239
- Guidelines and Limitations for CoPP, on page 239
- Default Settings for CoPP, on page 240
- Configuring CoPP, on page 241
- Verifying the CoPP Configuration, on page 243
- Displaying the CoPP Configuration Status, on page 243
- Monitoring CoPP, on page 244
- Clearing the CoPP Statistics, on page 245
- Additional References for CoPP, on page 245

Information About CoPP

Control Plane Policing (CoPP) protects the control plane and separates it from the data plane, which ensures network stability, reachability, and packet delivery.

This feature allows a policy map to be applied to the control plane. This policy map looks like a normal QoS policy and is applied to all traffic destined to any of the IP addresses of the router or Layer 3 switch. A common attack vector for network devices is the denial-of-service (DoS) attack, where excessive traffic is directed at the device interfaces.

The Cisco NX-OS device provides CoPP to prevent DoS attacks from impacting performance. Such attacks, which can be perpetrated either inadvertently or maliciously, typically involve high rates of traffic destined to the supervisor module or CPU itself.

The supervisor module divides the traffic that it manages into three functional components or planes:

**Data plane**

Handles all the data traffic. The basic functionality of a Cisco NX-OS device is to forward packets from one interface to another. The packets that are not meant for the switch itself are called the transit packets. These packets are handled by the data plane.
Control plane
Handles all routing protocol control traffic. These protocols, such as the Border Gateway Protocol (BGP) and the Open Shortest Path First (OSPF) Protocol, send control packets between devices. These packets are destined to router addresses and are called control plane packets.

Management plane
Runs the components meant for Cisco NX-OS device management purposes such as the command-line interface (CLI) and Simple Network Management Protocol (SNMP).

The supervisor module has both the management plane and control plane and is critical to the operation of the network. Any disruption or attacks to the supervisor module will result in serious network outages. For example, excessive traffic to the supervisor module could overload and slow down the performance of the entire Cisco NX-OS device. Another example is a DoS attack on the supervisor module that could generate IP traffic streams to the control plane at a very high rate, forcing the control plane to spend a large amount of time in handling these packets and preventing the control plane from processing genuine traffic.

Examples of DoS attacks are as follows:

- Internet Control Message Protocol (ICMP) echo requests
- IP fragments
- TCP SYN flooding

These attacks can impact the device performance and have the following negative effects:

- Reduced service quality (such as poor voice, video, or critical applications traffic)
- High route processor or switch processor CPU utilization
- Route flaps due to loss of routing protocol updates or keepalives
- Unstable Layer 2 topology
- Slow or unresponsive interactive sessions with the CLI
- Processor resource exhaustion, such as the memory and buffers
- Indiscriminate drops of incoming packets

Caution
It is important to ensure that you protect the supervisor module from accidental or malicious attacks by configuring control plane protection.

Control Plane Protection
To protect the control plane, the Cisco NX-OS device segregates different packets destined for the control plane into different classes. Once these classes are identified, the Cisco NX-OS device polices the packets, which ensures that the supervisor module is not overwhelmed.

Control Plane Packet Types
Different types of packets can reach the control plane:
Receive packets
Packets that have the destination address of a router. The destination address can be a Layer 2 address (such as a router MAC address) or a Layer 3 address (such as the IP address of a router interface). These packets include router updates and keepalive messages. Multicast packets can also be in this category where packets are sent to multicast addresses that are used by a router.

Exception packets
Packets that need special handling by the supervisor module. For example, if a destination address is not present in the Forwarding Information Base (FIB) and results in a miss, the supervisor module sends an ICMP unreachable packet back to the sender. Another example is a packet with IP options set.

Redirected packets
Packets that are redirected to the supervisor module. Features such as Dynamic Host Configuration Protocol (DHCP) snooping or dynamic Address Resolution Protocol (ARP) inspection redirect some packets to the supervisor module.

Glean packets
If a Layer 2 MAC address for a destination IP address is not present in the FIB, the supervisor module receives the packet and sends an ARP request to the host.

All of these different packets could be maliciously used to attack the control plane and overwhelm the Cisco NX-OS device. CoPP classifies these packets to different classes and provides a mechanism to individually control the rate at which the supervisor module receives these packets.

Classification for CoPP
For effective protection, the Cisco NX-OS device classifies the packets that reach the supervisor modules to allow you to apply different rate controlling policies based on the type of the packet. For example, you might want to be less strict with a protocol packet such as Hello messages but more strict with a packet that is sent to the supervisor module because the IP option is set.

Rate Controlling Mechanisms
Once the packets are classified, the Cisco NX-OS device has two different mechanisms to control the rate at which packets arrive at the supervisor module: policing and rate limiting.

Using hardware policers, you can define separate actions for traffic that conforms to or violates certain conditions. These actions can transmit the packet, mark down the packet, or drop the packet.

You can configure the following parameters for policing:

**Committed information rate (CIR)**
Desired bandwidth, specified as a bit rate.

**Committed burst (BC)**
Size of a traffic burst that can exceed the CIR within a given unit of time and not impact scheduling.

CoPP Extended Rate
Beginning with Cisco NX-OS Release 7.1(1)N1(1), you can configure an extended CoPP committed information rate (CIR) limit of up to 61,440 Kbps for each customized CoPP profile.

CoPP Class Maps
The following table shows the available class maps and their configurations.
### Table 19: Class Map Configurations and Descriptions

<table>
<thead>
<tr>
<th>Class Map</th>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map type control-plane match-any copp-system-class-arp</td>
<td>match protocol arp</td>
<td>Class matches all ARP packets.</td>
</tr>
<tr>
<td></td>
<td>match protocol nd</td>
<td>Class matches all ARP packets and ND (NA, NS, RA, and RS) packets.</td>
</tr>
<tr>
<td>class-map type control-plane match-any copp-system-class-bgp</td>
<td>match protocol bgp</td>
<td>Class matches all BGP packets.</td>
</tr>
<tr>
<td>class-map type control-plane match-any copp-system-class-bridging</td>
<td>match protocol bridging</td>
<td>Class matches all STP and RSTP frames.</td>
</tr>
<tr>
<td>class-map type control-plane match-any copp-system-class-cdp</td>
<td>match protocol cdp</td>
<td>Class matches all CDP frames.</td>
</tr>
<tr>
<td>class-map type control-plane match-any copp-system-class-default</td>
<td>match protocol default</td>
<td>Class matches all frames. Used for the default policer.</td>
</tr>
<tr>
<td>class-map type control-plane match-any copp-system-class-dhcp</td>
<td>match protocol dhcp</td>
<td>Class matches all IPv4 DHCP packets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Class matches all both IPv4 DHCP packets.</td>
</tr>
<tr>
<td>class-map type control-plane match-any copp-system-class-eigrp</td>
<td>match protocol eigrp</td>
<td>Class matches all IPv4 EIGRP packets.</td>
</tr>
<tr>
<td></td>
<td>match protocol eigrp6</td>
<td>Class matches both IPv4 and IPv6 EIGRP packets.</td>
</tr>
<tr>
<td>class-map type control-plane match-any copp-system-class-exception</td>
<td>match protocol exception</td>
<td>Class matches all IP packets that are treated as exception packets (except TTL exception, IP Fragment exception and Same Interface exception packets) for IP routing purposes, such as packets with a Martian destination address or with an MTU failure.</td>
</tr>
<tr>
<td>class-map type control-plane match-any copp-system-class-excp-ip-frag</td>
<td>match protocol ip_frag</td>
<td>Class matches all IP packets that are fragments. (These packets are treated as exception packets from an IP routing perspective).</td>
</tr>
<tr>
<td>class-map type control-plane match-any copp-system-class-excp-same-if</td>
<td>match protocol same-if</td>
<td>Class matches all IP packets that are treated as exception packets for IP routing. The packets are matched because they are received from the interface where their destination is supposed to be.</td>
</tr>
<tr>
<td>Class Map</td>
<td>Configuration</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol ttl</td>
<td>Class matches all packets that are</td>
</tr>
<tr>
<td>copp-system-class-excp-ttl</td>
<td></td>
<td>treated as TTL exception packets (when TTL is 0) from a IP routing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>perspective.</td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol fip</td>
<td>Class matches all packets belonging to the FCoE Initialization Protocol.</td>
</tr>
<tr>
<td>copp-system-class-fip</td>
<td></td>
<td></td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol glean</td>
<td></td>
</tr>
<tr>
<td>copp-system-class-glean</td>
<td></td>
<td></td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol hsrp_vrrp</td>
<td>Class matches HSRP and VRRP packets.</td>
</tr>
<tr>
<td>copp-system-class-hsrp-vrrp</td>
<td>match protocol hsrp6</td>
<td>Class matches IPv4 HSRP, VRRP and IPv6 HSRP packets</td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol icmp_echo</td>
<td>Class matches all ICMP Echo (Ping) packets.</td>
</tr>
<tr>
<td>copp-system-class-icmp-echo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol igmp</td>
<td>Class matches all IGMP packets.</td>
</tr>
<tr>
<td>copp-system-class-igmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol isis_dce</td>
<td></td>
</tr>
<tr>
<td>copp-system-class-isis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol unicast</td>
<td>Class matches all unicast routed packets that did not find a destination</td>
</tr>
<tr>
<td>copp-system-class-l3dest-miss</td>
<td></td>
<td>in the FIB.</td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol lacp</td>
<td>Class matches all Link Aggregation Control Protocol (LACP) frames.</td>
</tr>
<tr>
<td>copp-system-class-lacp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol lldp_dcx</td>
<td>Class matches all LLDP frames.</td>
</tr>
<tr>
<td>copp-system-class-lldp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol mcast_last_hop</td>
<td>Class matches all IP multicast last hop packets.</td>
</tr>
<tr>
<td>copp-system-class-mcast-miss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol multicast</td>
<td>Class matches all IP multicast frames that could not be routed because</td>
</tr>
<tr>
<td>copp-system-class-mcast-miss</td>
<td></td>
<td>they did not have an entry in the FIB.</td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol mgmt</td>
<td>Class matches all management-related frames, such as SNMP, HTTP, NTP,</td>
</tr>
<tr>
<td>copp-system-class-mgmt</td>
<td></td>
<td>Telnet, and SSH.</td>
</tr>
<tr>
<td>class-map type control-plane match-any</td>
<td>match protocol msdp</td>
<td>Class matches MSDP packets.</td>
</tr>
<tr>
<td>copp-system-class-msdp</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### CoPP Policy Templates

When you bring up your Cisco NX-OS device for the first time, the Cisco NX-OS software installs the default copp-system-policy to protect the supervisor module from DoS attacks. You can choose the CoPP policy template for your deployment scenario by specifying CoPP policy options from the initial setup utility:

- **Default CoPP Policy** (copp-system-policy-default)
- **Scaled Layer 2 CoPP Policy** (copp-system-policy-scaled-l2)
- **Scaled Layer 3 CoPP Policy** (copp-system-policy-scaled-l3)
- **Customized CoPP Policy** (copp-system-policy-customized)

If you do not select an option or choose not to execute the setup utility, the Cisco NX-OS software applies the Default policing. Cisco recommends starting with the default policy and later modifying the CoPP policies as required.

The default copp-system-policy-default policy has optimized values suitable for basic device operations.

You can change which CoPP policy is used by using the `service-policy input policy-name` command in the control plane configuration mode.

#### Default CoPP Policy

The copp-system-policy-default policy is applied to the switch by default. It has the classes with policer rates that should suit most network installations. You cannot modify this policy or the class maps associated with it. In addition, you cannot modify the class map configurations in this policy.
This policy has the following configuration:

```
policy-map type control-plane copp-system-policy-default
  class copp-system-class-igmp
    police cir 1024 kbps bc 65535 bytes
  class copp-system-class-pim-hello
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-bridging
    police cir 20000 kbps bc 4800000 bytes
  class copp-system-class-arp
    police cir 1024 kbps bc 3600000 bytes
  class copp-system-class-dhcp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-mgmt
    police cir 12000 kbps bc 4800000 bytes
  class copp-system-class-lacp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-lldp
    police cir 2048 kbps bc 4800000 bytes
  class copp-system-class-udp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-isis
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-msdp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-cdp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-fip
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-bgp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-eigrp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-exception
    police cir 64 kbps bc 4800000 bytes
  class copp-system-class-glean
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-harp-vrrp
    police cir 1024 kbps bc 256000 bytes
  class copp-system-class-icmp-echo
    police cir 64 kbps bc 3600000 bytes
  class copp-system-class-opf
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-pim-register
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-rip
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-l3dest-miss
    police cir 64 kbps bc 256000 bytes
  class copp-system-class-mcast-miss
    police cir 256 kbps bc 3200000 bytes
  class copp-system-class-excp-ip-frag
    police cir 64 kbps bc 3200000 bytes
  class copp-system-class-excp-same-if
    police cir 64 kbps bc 3200000 bytes
  class copp-system-class-excp-ttl
    police cir 64 kbps bc 3200000 bytes
  class copp-system-class-default
    police cir 512 kbps bc 6400000 bytes
```
Scaled Layer 2 CoPP Policy

The copp-system-policy-scaled policy has most classes with policer rates that are same as the default policy. However, it has higher policer rates for IGMP and ISIS. You cannot modify this policy or the class maps associated with it. In addition, you cannot modify the class map configurations in this policy.

This policy has the following configuration:

```plaintext
policy-map type control-plane copp-system-policy-scaled-l2
  class copp-system-class-igmp
    police cir 4096 kbps bc 264000 bytes
  class copp-system-class-pim-hello
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-bridging
    police cir 20000 kbps bc 4800000 bytes
  class copp-system-class-arp
    police cir 1024 kbps bc 3600000 bytes
  class copp-system-class-dhcp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-mgmt
    police cir 12000 kbps bc 4800000 bytes
  class copp-system-class-lacp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-lldp
    police cir 2048 kbps bc 4800000 bytes
  class copp-system-class-udld
    police cir 2048 kbps bc 4800000 bytes
  class copp-system-class-isis
    police cir 2048 kbps bc 4800000 bytes
  class copp-system-class-msdp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-cdp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-fip
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-bgp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-eigrp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-exception
    police cir 64 kbps bc 4800000 bytes
  class copp-system-class-glean
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-hsrp-vrrp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-icmp-echo
    police cir 64 kbps bc 3600000 bytes
  class copp-system-class-ospf
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-pim-register
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-rip
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-l3dest-miss
    police cir 64 kbps bc 3200000 bytes
  class copp-system-class-mcast-miss
    police cir 256 kbps bc 3200000 bytes
  class copp-system-class-excp-ip-frag
    police cir 64 kbps bc 3200000 bytes
  class copp-system-class-excp-same-if
    police cir 64 kbps bc 3200000 bytes
  class copp-system-class-excp-ttl
```
Scaled Layer 3 CoPP Policy

The copp-system-policy-scaled-l3 policy has most classes with policer rates that are same as the default policy. However, it has higher policer rates for IGMP, ICMP Echo, ISIS, Mcast-miss, and Glean related classes. You cannot modify this policy or the class maps associated with it. In addition, you cannot modify the class map configurations in this policy.

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy-scaled-l3
  class copp-system-class-igmp
    police cir 4096 kbps bc 264000 bytes
  class copp-system-class-pim-hello
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-bridging
    police cir 20000 kbps bc 4800000 bytes
  class copp-system-class-arp
    police cir 4000 kbps bc 3600000 bytes
  class copp-system-class-dhcp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-mgmt
    police cir 12000 kbps bc 4800000 bytes
  class copp-system-class-lacp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-lldp
    police cir 2048 kbps bc 4800000 bytes
  class copp-system-class-isis
    police cir 2048 kbps bc 4800000 bytes
  class copp-system-class-msdp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-cdp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-fip
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-bgp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-eigrp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-exception
    police cir 64 kbps bc 4800000 bytes
  class copp-system-class-glean
    police cir 4000 kbps bc 4800000 bytes
  class copp-system-class-harp-rrp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-icmp-echo
    police cir 4000 kbps bc 3600000 bytes
  class copp-system-class-ospf
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-pim-register
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-rip
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-l3dest-miss
    police cir 64 kbps bc 3200000 bytes
  class copp-system-class-mcast-miss
```
Customizable CoPP Policy

The copp-system-policy-customized policy is configured identically to the default policy, but can be customized for different class map information rates and burst sizes.

You cannot add or delete any of the class maps configured in this policy.

Important

This policy is meant for advanced users. We recommend that you use extreme caution when configuring this policy and test it extensively before deploying it in your production network.

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy-customized
  class copp-system-class-igmp
    police cir 1024 kbps bc 65535 bytes
  class copp-system-class-pim-hello
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-bridging
    police cir 20000 kbps bc 4800000 bytes
  class copp-system-class-arp
    police cir 1024 kbps bc 3600000 bytes
  class copp-system-class-dhcp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-mgmt
    police cir 12000 kbps bc 4800000 bytes
  class copp-system-class-lacp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-lldp
    police cir 2048 kbps bc 4800000 bytes
  class copp-system-class-udld
    police cir 2048 kbps bc 4800000 bytes
  class copp-system-class-isis
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-msdp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-cdp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-fip
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-bgp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-eigrp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-exception
    police cir 64 kbps bc 4800000 bytes
  class copp-system-class-glean
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-hsrp-vrrp
```
CoPP and the Management Interface

The Cisco NX-OS device supports only hardware-based CoPP which does not support the management interface (mgmt0). The out-of-band mgmt0 interface connects directly to the CPU and does not pass through the in-band traffic hardware where CoPP is implemented.

On the mgmt0 interface, ACLs can be configured to give or deny access to a particular type of traffic.

Licensing Requirements for CoPP

This feature does not require a license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide.

Guidelines and Limitations for CoPP

- CoPP is a feature that is enabled by default in the switch. You cannot enable or disable CoPP.
- Only one control-plane policy can be applied at a time.
- Removing a CoPP policy applies the default CoPP policy. In this way, a CoPP policy is always applied.
- You cannot add or delete any classes or policies.
- You cannot change the order of the classes or remove a class from any policy.
- You cannot modify the default, the Scaled Layer-2, or the Scaled Layer 3 policies. However, you can modify the information rate and burst size of the classes in the customized policy.
- The customized policy configuration is the same as the default policy configuration, unless the customized policy has been modified.
When upgrading from a previous release, the default CoPP policy is enabled by default on the switch.

After modifying the customized policy or changing the applied policy, the statistical counters are reset.

After you perform an ISSU, the statistical counters are reset.

Cisco recommends that you use the default CoPP policy initially and then later determine which of the CoPP policies to use based on the data center and application requirements.

Customizing CoPP is an ongoing process. CoPP must be configured according to the protocols and features used in your specific environment as well as the supervisor features that are required by the server environment. As these protocols and features change, CoPP must be modified.

Cisco recommends that you continuously monitor CoPP. If drops occur, determine if CoPP dropped traffic unintentionally or in response to a malfunction or attack. In either event, analyze the situation and evaluate the need to use a different CoPP policy or modify the customized CoPP policy.

All the traffic that you do not specify in the other class maps is put into the last class, the default class.

The Cisco NX-OS software does not support egress CoPP or silent mode. CoPP is supported only on ingress (you cannot use the service-policy output copp command to the control plane interface).

When a packet meets multiple exception conditions, CoPP matches the packet based on the order in which the CoPP ACLs are configured and match it only against a single class. This is an expected CoPP behavior.

The copp-system-class-exception matches all IP data packets that are treated as exception packets (except TTL exception, IP Fragment exception and Same Interface exception packets) since the hardware itself is not capable of processing them. Control packets with ip-options are supposed to be caught by the respective protocol class and the protocol stack running on the switch is usually able to process them.

If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

**Default Settings for CoPP**

This table lists the default settings for CoPP parameters.

**Table 20: Default CoPP Parameters Settings**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default policy</td>
<td>9 policy entries</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The maximum number of supported policies with associated class maps is 128.</td>
</tr>
</tbody>
</table>
Configuring CoPP

Applying a CoPP Policy to the Switch

You can apply one of the following CoPP policies to the switch:

- Default CoPP Policy (`copp-system-policy-default`).
- Scaled Layer 2 CoPP Policy (`copp-system-policy-scaled-l2`).
- Scaled Layer 3 CoPP Policy (`copp-system-policy-scaled-l3`).
- Customized CoPP Policy (`copp-system-policy-customized`).

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>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters control-plane mode.</td>
</tr>
<tr>
<td>switch(config) # control-plane</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Applies the specified CoPP policy map. The <code>policy-map-name</code> can be <code>copp-system-policy-default</code>, <code>copp-system-policy-scaled-l2</code>, <code>copp-system-policy-scaled-l3</code>, or <code>copp-system-policy-customized</code>.</td>
</tr>
<tr>
<td>switch(config-cp) # service-policy input policy-map-name</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
<tr>
<td>switch(config-cp) # copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Example

This example shows how to apply a CoPP policy to the device:

```
switch# configure terminal
switch(config)# control-plane
switch(config-cp) # service-policy input copp-system-policy-default
switch(config-cp) # copy running-config startup-config
```

Modifying the Customized CoPP Policy

You can only modify the information rates and burst sizes of the class maps configured in this policy.
### Configuring CoPP Extended Rate

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> switch(config)# control-plane</td>
<td>Enters control-plane mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> (Optional) switch(config-cp)# service-policy input copp-system-policy-customized</td>
<td>Applies the customized CoPP system policy map.</td>
</tr>
<tr>
<td><strong>Step 4</strong> switch(config-cp)# ingress-copp</td>
<td>Allows CoPP extended CIR configuration.</td>
</tr>
<tr>
<td><strong>Step 5</strong> switch(config-cp)# policy-map type control-plane copp-system-policy-customized</td>
<td>Enters configuration mode for the customized CoPP policy.</td>
</tr>
</tbody>
</table>

### Example

This example shows how to modify the customized CoPP policy:

```
switch(config)# policy-map type control-plane copp-system-policy-customized
switch(config-pmap)# class copp-system-class-bridging
switch(config-pmap-c)# police cir 10000 kbps bc 2400000 bytes
```

---

### Configuring Control Plane Policing

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> switch(config)# policy-map type control-plane copp-system-policy-customized</td>
<td>Enters configuration mode for the customized CoPP policy.</td>
</tr>
<tr>
<td><strong>Step 3</strong> switch(config-pmap)# class class-map-name</td>
<td>Specifies one of the 28 predefined class-maps listed in any CoPP predefined policy.</td>
</tr>
<tr>
<td><strong>Step 4</strong> switch(config-pmap-c)# police cir rate-value kbps bc buffer-size bytes</td>
<td>Configures the committed information rate (CIR) and committed burst size (BC). The range for cir is from 1 to 20480. The range for bc is from 1500 to 6400000.</td>
</tr>
<tr>
<td><strong>Step 5</strong> switch(config-pmap-c)# copy running-config startup-config</td>
<td>Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

---

Example

This example shows how to modify the customized CoPP policy:

```
switch(config)# policy-map type control-plane copp-system-policy-customized
switch(config-pmap)# class copp-system-class-bridging
switch(config-pmap-c)# police cir 10000 kbps bc 2400000 bytes
```
# Purpose

### Command or Action

**Step 6**

`switch(config-pmap)# class class-map-name`

Specifies one of the 28 predefined class-maps listed in any CoPP predefined policy.

**Step 7**

`switch(config-pmap-c)# police cir rate-value kbps bc buffer-size bytes`

Configures the committed information rate (CIR) and committed burst size (BC). The range for extended CIR is from 1 to 61,440 Kbps. The range for BC is from 1500 to 6400000.

**Step 8**

`switch(config-pmap-c)# copy running-config startup-config`

Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

---

## Example

This example shows how to configure CoPP Extended Rate:

```bash
switch(config)# control-plane
switch(config-cp)# ingress-copp
switch(config-cp)# policy-map type control-plane copp-system-policy-customized
switch(config-pmap)# class copp-system-class-lacp
switch(config-pmap-c)# police cir 51200 kbps bc 4800000 bytes
```

---

## Verifying the CoPP Configuration

Use one of the following commands to verify the configuration:

### Command

**Purpose**

- `show policy-map type control-plane [expand] [name policy-map-name]`
  
  Displays the control plane policy map with associated class maps.

- `show policy-map interface control-plane`
  
  Displays the policy values with associated class maps and drops per policy or class map.

- `show class-map type control-plane [class-map-name]`
  
  Displays the control plane class map configuration, including the ACLs that are bound to this class map.

---

## Displaying the CoPP Configuration Status

### Procedure

**Step 1**

`switch# show copp status`

Displays the configuration status for the CoPP feature.
Example
This example shows how to display the CoPP configuration status:

```
switch# show copp status
```

Monitoring CoPP

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> switch# show policy-map interface control-plane</td>
<td>Displays packet-level statistics for all classes that are part of the applied CoPP policy. Statistics are specified in terms of OutPackets (packets admitted to the control plane) and DropPackets (packets dropped because of rate limiting).</td>
</tr>
</tbody>
</table>

Example
This example shows how to monitor CoPP:

```
switch# show policy-map interface control-plane
Control Plane

service-policy input: copp-system-policy-default

class-map copp-system-class-igmp (match-any)
 match protocol igmp
 police cir 1024 kbps , bc 65535 bytes
 conformed 0 bytes; action: transmit
 violated 0 bytes;
class-map copp-system-class-pim-hello (match-any)
 match protocol pim
 police cir 1024 kbps , bc 4800000 bytes
 conformed 0 bytes; action: transmit
 violated 0 bytes;
....
```
Clearing the CoPP Statistics

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>(Optional) switch# show policy-map interface control-plane</td>
<td>Displays the currently applied CoPP policy and per-class statistics.</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch# clear copp statistics</td>
<td>Clears the CoPP statistics.</td>
</tr>
</tbody>
</table>

Example

This example shows how to clear the CoPP statistics for your installation:

switch# show policy-map interface control-plane
switch# clear copp statistics

Additional References for CoPP

This section provides additional information related to implementing CoPP.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing</td>
<td>Cisco NX-OS Licensing Guide</td>
</tr>
<tr>
<td>Command reference</td>
<td></td>
</tr>
</tbody>
</table>
Configuring TCAM Carving

This chapter contains the following sections:

• Information About TCAM Carving, on page 247
• Information About User-Defined Templates, on page 247
• Creating a User-Defined Template, on page 250
• Modifying a User Defined Template, on page 251
• Committing a User-Defined Template, on page 251
• Deleting a Template, on page 252
• Verifying the TCAM Carving Configuration, on page 253

Information About TCAM Carving

The Ternary Content-Addressable Memory (TCAM) carving feature uses a template-based approach that enables you to modify the default region sizes of the TCAM. When the switch boots up, you see this default template, unless you have configured any other template. This table lists the types and sizes of various regions in a template.

Information About User-Defined Templates

In addition to the default template, you can create a maximum of 16 templates (which means that you can have 17 templates at one time). You can specify whatever sizes of ternary content addressable memory (TCAM) regions you want.

You can apply the following operations on each template:

• Create
• Modify
• Delete
• Commit

Each template can be in one of the following states:

• Saved
• Committed
Create

When you create a template, the size of the TCAM regions are initialized to the default values. When a template is created, the template is in the saved state by default. Once you create a template, you can modify it to change the size of any TCAM region. You should configure the size of the region in multiples of 64 because the size of each TCAM block is 64 entries. If you enter a value that is not a multiple of 64, an error message asks you to enter the value again.

Modify

You can modify any saved template to change the size of any TCAM region but you cannot modify the size of any region in the TCAM to 0. During the modification, the software checks that the size that you entered is on a 64 boundary. When you modify a template, the combined size of all the TCAM regions might have fewer than 4096 entries. During a modification, the software does not check that you have fewer than 4096 entries.

You can modify a template only when it is in the saved state. After a template is committed, you cannot modify it.

A user-defined committed template can be changed to the created state by servicing another user-defined template or default template.

To service another user-defined template, enter the following command:

```
hardware profile tcam resource service-template user-defined-template
```

To service a default template, enter the following command:

```
no hardware profile tcam resource service-template currently-committed-template
```

Delete

You can delete any saved template. After you delete a template, all information about the template is lost. A committed template cannot be deleted.

A user-defined committed template can be changed to the created state by servicing another user-defined template or default template.

To service another user-defined template, enter the following command:

```
hardware profile tcam resource service-template user-defined-template
```

To service a default template, enter the following command:

```
no hardware profile tcam resource service-template currently-committed-template
```

Commit

You can commit any of your user-defined templates or the default template that is provided by the software. To commit a template, enter the `commit` command and perform a reboot of the switch. When you enter the `commit` command, the software validates the template. If the validation is successful, the software prompts you to reboot the switch. The template (user defined or default) is applied after the reboot. If you did not choose to reboot, no changes are made to the TCAM regions and no template is committed.

From Cisco NX-OS Release 7.1(4)N1(1) onwards, after you commit a template, the system prompts you whether to proceed with copying the running configuration to the startup configuration and rebooting the switch. After you agree to continue, the following occurs:

- The committed template is saved in the startup configuration.
• The switch is rebooted.
• The committed template is used by the software.
• The template goes to the running state.

Prior to Cisco NX-OS Release 7.1(4)N1(1), after you commit a template, the system does not automatically reboot but a message is displayed in the `commit` command output asking you to reboot the switch for the committed template to take effect.

**Note**

If you perform a write erase, reload, and copy running configuration from a back-up configuration containing uncommitted TCAM profile, the following occurs:

1. After the TCAM profile is committed, switch automatically reloads without any prompt.
2. Any configuration after TCAM carving CLI is not applied.
3. To restore configuration with the committed TCAM profile, you need to copy backup configuration to running configuration again. However, there is no switch reload as the TCAM carving profile is already committed.

When the switch is reloaded due to the new committed TCAM profile, the `show system reset-reason` command displays the reason for the reload as shown below:

```
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 302777 usecs after Sun Jan 20 22:02:37 2016
   Reason: **Reload due to change in TCAM service-template**
   Service:
   Version: 7.1(4)N1(1)

2) At 314447 usecs after Sun Jan 20 21:52:58 2016
   Reason: **Reset Requested by CLI command reload**
   Service:
   Version: 7.1(4)N1(1)

3) At 20142 usecs after Sun Jan 20 21:27:33 2016
   Reason: **Reset Requested by CLI command reload**
   Service:
   Version: 7.1(4)N1(1)
```

After the switch reboots, the committed template is applied to all ASICs on the Cisco Nexus device. You cannot commit different templates to different ASICs on the Cisco Nexus device. All saved templates and committed templates along with the size of each region of each template are displayed in the running configuration.

When a template is committed, the software checks the following:

1. The combined size of all regions in the TCAM is 4096 entries.
2. The size of each region fits within the TCAM. At any point of time, there is always a running size for the TCAM region. This running size (the current size in the hardware TCAM) is defined by either the default or a user-defined template that was committed and is currently being used as the running template. If you increase the size of a region in a template that is currently being committed, from the current running size, the software checks if there are enough free entries outside the current region (entries that are not allocated to any other region) that can be used to increase the size of the region. If you decrease the size of a region
in a template that is currently being committed from the current running size, the software checks to
determine if there are enough free entries within the region that can be freed up to reduce the size of the
TCAM region. All changes that reduce the sizes of the regions within the template are done before the
changes to increase the sizes of regions within the template.

3. The hardware does not support more than 256 entries in the supervisor region and span regions. This
check is done during validation.

If all these checks pass, you can commit the template and you are prompted to apply the template by rebooting.
If these checks fail, the commit fails and the template goes back to the saved state. If the commit fails, the
commit command output displays the reasons that it failed.

You cannot modify or delete the default template. You can only move this template from saved to committed
or committed to saved. If the default template is committed, it is not displayed in the running configuration.
To apply the default template, enter the no commit command using the currently running template. Entering
this command executes the same validation checks that were performed when you committed the template.
If all validations succeed, the software prompts you to reboot the switch. If you agree to reboot, the template
is saved in the startup configuration and the system is rebooted. After the reboot, the default template is
applied. The startup configuration has the committed template that you committed before rebooting. After
rebooting, the template in the startup configuration is used. If there is no committed template in the startup
configuration, the default template is used.

You create and manage the TCAM carving templates by entering the template manager commands. The
template-based TCAM carving CLI is supported in config-sync. Only template creation is supported inside
config-sync. Template commit should be performed separately on each switch outside the config-sync context.

Creating a User-Defined Template

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# hardware profile tcam resource template template-name</td>
<td>Creates a new template with the default region sizes. A maximum of 16 templates (plus the default) can be created. The template-name argument can be a maximum of 64 characters.</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to create a user-defined template named qos-template:

```
switch# configure terminal
switch(config)# hardware profile tcam resource template qos-template
```
# Modifying a User Defined Template

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# hardware profile tcam resource template template-name</td>
<td>Creates a new template with the default region sizes. A maximum of 16 templates (plus the default) can be created. Use this command to enter template mode.</td>
</tr>
</tbody>
</table>

## Example

This example shows how to modify a user-defined qos template.

```
switch# configure terminal
switch(config)# hardware profile tcam resource template qos-template
switch(config-tmpl) qos 64
```

# Committing a User-Defined Template

You can commit a user-defined template.

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Required: switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# hardware profile tcam resource service-template template-name</td>
<td>Commits a previously defined template in the running image. After you commit a template, the system prompts you whether to proceed with copying the running configuration to the startup configuration and rebooting the switch. If you agree to continue, the specified template is applied after the reboot. Otherwise, no changes are made to the TCAM regions and no template is committed.</td>
</tr>
</tbody>
</table>
| Step 3 | (Optional) switch# show hardware profile tcam resource template | Displays all templates.  
**Note** After the switch reloads, use this command to display the committed template. |
Example

This example shows how to commit a user-defined template:

```
switch# configure terminal
switch(config)# hardware profile tcam resource service-template temp1
```

Details of the temp1 template you are trying to commit are as follows:

```
Template name: temp1
Current state: Created
```

<table>
<thead>
<tr>
<th>Region</th>
<th>Features</th>
<th>Size-allocated</th>
<th>Current-size</th>
<th>Current-usage</th>
<th>Available/free</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vacl</td>
<td>Vacl</td>
<td>1024</td>
<td>1024</td>
<td>15</td>
<td>1009</td>
</tr>
<tr>
<td>Ifacl</td>
<td>Ifacl</td>
<td>1152</td>
<td>1152</td>
<td>209</td>
<td>943</td>
</tr>
<tr>
<td>Rbacl</td>
<td>Rbacl</td>
<td>1152</td>
<td>1152</td>
<td>3</td>
<td>1149</td>
</tr>
<tr>
<td>Qos</td>
<td>Qos</td>
<td>448</td>
<td>448</td>
<td>30</td>
<td>418</td>
</tr>
<tr>
<td>Span</td>
<td>Span</td>
<td>64</td>
<td>64</td>
<td>2</td>
<td>62</td>
</tr>
<tr>
<td>Sup</td>
<td>Sup</td>
<td>256</td>
<td>256</td>
<td>58</td>
<td>198</td>
</tr>
</tbody>
</table>

To finish committing the template, the system will do the following:

1> Save running config: "copy running-config startup-config"
2> Reboot the switch: "reload"

Do you really want to continue with RELOAD? (y/n) [no] yes
System is still initializing
Configuration mode is blocked until system is ready
switch(config)# [16152.925385] Shutdown Ports...
[16152.959744] writing reset reason 9
[snip]

/AFTER SWITCH RELOADS/

```
switch# show hardware profile tcam resource template
```

<table>
<thead>
<tr>
<th>Template</th>
<th>Type</th>
<th>State</th>
<th>Vacl</th>
<th>Ifacl</th>
<th>Rbacl</th>
<th>Qos</th>
<th>Span</th>
<th>Sup</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>system</td>
<td>Created</td>
<td>1024</td>
<td>1152</td>
<td>1152</td>
<td>448</td>
<td>64</td>
<td>256</td>
<td>4096</td>
</tr>
<tr>
<td>temp1</td>
<td>user</td>
<td>Committed</td>
<td>1024</td>
<td>1152</td>
<td>1152</td>
<td>448</td>
<td>64</td>
<td>256</td>
<td>4096</td>
</tr>
<tr>
<td>temp2</td>
<td>user</td>
<td>Created</td>
<td>1024</td>
<td>1152</td>
<td>1152</td>
<td>448</td>
<td>64</td>
<td>256</td>
<td>4096</td>
</tr>
</tbody>
</table>

Deleting a Template

After creating a template, the template can be deleted. Deleting removes all the information about the template from the software.
## Verifying the TCAM Carving Configuration

To display TCAM carving configuration information, enter one of the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show hardware profile tcam resource template</code></td>
<td>Displays all templates.</td>
</tr>
<tr>
<td><code>show hardware profile tcam resource template name template-name</code></td>
<td>Displays a user-defined template.</td>
</tr>
<tr>
<td><code>show hardware profile tcam resource template default</code></td>
<td>Displays a default template.</td>
</tr>
</tbody>
</table>
CHAPTER 14

Configuring Sup-region TCAM Monitoring

This chapter contains the following sections:

- Information About Sup-region TCAM Monitoring, on page 255
- Licensing Requirements for Sup-region TCAM Monitoring, on page 256
- Guidelines and Limitations for Sup-region TCAM Monitoring, on page 256
- Default Setting for Sup-region TCAM Monitoring, on page 256
- Configuring Sup-region TCAM Monitoring, on page 257
- Verifying Sup-region TCAM Monitoring, on page 260
- Configuration Examples for Sup-region TCAM Monitoring, on page 260
- Additional References for Sup-region TCAM Monitoring, on page 260
- Feature History for Sup-region TCAM Monitoring, on page 261

Information About Sup-region TCAM Monitoring

The Sup-region Ternary Content-Addressable Memory (TCAM) Monitoring feature is a monitoring mechanism that enables detection, reporting and correction of sup-region TCAM entry corruption. This monitoring mechanism provides the following functionalities:

- Detection—Checks for corruptions in any sup-region TCAM entry and reports it.
- Correction—Provides corrective mechanism to rewrite the corrupted sup-region TCAM entry.

On-demand Detection of Corrupted Sup-region TCAM Entries

Use the `hardware sup-tcam monitoring trigger-detection` command to verify if any sup-region TCAM entry is corrupted. This command triggers a verification iteration that involves reading each sup-region TCAM entry and comparing this TCAM entry data with the stored content.

Periodic Detection of Corrupted Sup-region TCAM Entries

By default, the periodic sup-region TCAM entry corruption detection mechanism is disabled. Use the `hardware sup-tcam monitoring enable` command to enable periodic sup-region TCAM entry corruption detection. By default, the periodic corruption detection mechanism is set to run once every 1440 minutes or 1 day.
A syslog is generated if any sup-region TCAM entry is found to be corrupt. This syslog entry has details about the TCAM entry index, ASIC and slot number.

**In-Service Software Upgrades and In-Service Software Downgrades**

The sup-region TCAM entry monitoring mechanism tracks the content of the programmed TCAM entry by storing the TCAM entry content in the Persistent Storage Service (PSS). After a non-disruptive In-Service Software Upgrade (ISSU), this content is restored for verification. Before an ISSU is done, all configurations will be stored in the PSS. Statistics are not stored in the PSS.

You cannot restore a sup-region TCAM entry after a non-disruptive ISSU from a Cisco NX-OS version on which sup-region TCAM monitoring is not supported to a Cisco NX-OS version on which sup-region TCAM monitoring is supported. During such a scenario, syslogs are not generated for any corrupted sup-region TCAM entries and all commands related to sup-region TCAM monitoring will be disabled. You have to then reload the switch to trigger sup-region TCAM monitoring.

The Sup-region TCAM Monitoring feature does not support In-Service Software Downgrade (ISSD). Disable the Sup-region TCAM Monitoring feature before performing an ISSD.

**Licensing Requirements for Sup-region TCAM Monitoring**

The following table shows the licensing requirements for this feature:

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>Sup-region TCAM Monitoring requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the License and Copyright Information for Cisco NX-OS Software.</td>
</tr>
</tbody>
</table>

**Guidelines and Limitations for Sup-region TCAM Monitoring**

- The sup-region TCAM entry at 3844 is not verified during detection of corrupted sup-region TCAM entries.
- Reload the switch to trigger sup-region TCAM monitoring after a non-disruptive ISSU from a Cisco NX-OS version on which sup-region TCAM Monitoring is not supported to a Cisco NX-OS version on which sup-region TCAM Monitoring is supported.
- ISSD is not supported.

**Default Setting for Sup-region TCAM Monitoring**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sup-region TCAM Monitoring</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Configuring Sup-region TCAM Monitoring

Configuring On-Demand Detection of Corrupted Sup-region TCAM Entries

Procedure

Step 1 Trigger a verification iteration that involves reading each sup-region TCAM entry and comparing this TCAM entry data with the stored content:

switch# hardware sup-tcam monitoring trigger-detection

Note A syslog is generated if there is a mismatch.

Step 2 (Optional) Display details about sup-region TCAM monitoring:

switch# show platform afm info sup-tcam monitoring info

Running Configuration

This example shows how to enable on-demand detection of corrupted sup-region TCAM entries, followed by a verification command that displays the sup-region TCAM monitoring details.

hardware sup-tcam monitoring trigger-detection

switch# show platform afm info sup-tcam monitoring info

SUP TCAM Monitoring Info

------------------------
Periodic Monitoring Status : Disabled
Timer expiry : 0 minutes
Number of iterations run : 0
Last iteration run at : --
SUP TCAM corruption detected : NO
Feasibility : Feasible
DB Restore status : Restored

Configuring Periodic Detection of Corrupted Sup-region TCAM Entries

Procedure

Step 1 Enter global configuration mode:

switch# configure terminal

Step 2 Required: Enable a continuous periodic detection of corrupted sup-region TCAM entries:
Correcting the Corrupted Sup-region TCAM Entries

Procedure

**Step 1** Rewrite a corrupted sup-region TCAM entry content with the stored content:

```
switch# hardware sup-tcam correction asic {ASIC-ID | all} entry {TCAM-INDEX | all}
```

**Step 2** (Optional) Display write access statistics per TCAM entry per ASIC per slot, along with the number of writes, clears and timestamps of the writes and clears since the previous switch reload:

```
switch# show access statistics [asic {ASIC-ID | all}] [tcam-index {TCAM-INDEX | all}]
```
Running Configuration

This example shows how to correct a corrupted sup-region TCAM entry, followed by verification commands that display the write access statistics per TCAM entry per ASIC per slot, along with the number of writes, clears and timestamps of the writes and clears since the previous switch reload. Replace the placeholders with relevant values for your setup.

```
switch# show platform afm info tcam access stats [ASIC-ID]

```

Hardware sup-tcam correction asic <2> entry <5>
*
*
switch# show platform afm info tcam access stats <2>

*NA - Not Available

<table>
<thead>
<tr>
<th>Slot/Asic</th>
<th>ASIC ID</th>
<th>TCAM Index</th>
<th>Writes</th>
<th>Clears</th>
<th>Corrupt</th>
<th>Last Operation</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>NA</td>
<td>Clear</td>
<td>Tue Aug 16 06:43:12</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>NA</td>
<td>Clear</td>
<td>Tue Aug 16 06:43:12</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>122</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>123</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>124</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>125</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>126</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>127</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>128</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>129</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>130</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>131</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>132</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>133</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>134</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>135</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>136</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>137</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>138</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
<tr>
<td>0/2 2016</td>
<td>2</td>
<td>139</td>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>Write</td>
<td>Tue Aug 16 07:10:33</td>
</tr>
</tbody>
</table>
Verifying Sup-region TCAM Monitoring

To display sup-region TCAM monitoring information, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show platform afm info sup-tcam monitoring info</code></td>
<td>Display details about sup-region TCAM monitoring.</td>
</tr>
<tr>
<td><code>show platform afm info tcam access stats [ASIC-ID]</code></td>
<td>Display write access statistics per TCAM entry per ASIC per slot, along with the number of writes, clears and timestamps of the writes and clears since the previous switch reload.</td>
</tr>
</tbody>
</table>

Configuration Examples for Sup-region TCAM Monitoring

This section provides configuration examples for sup-region TCAM Monitoring.

**Configuring On-Demand Detection of Corrupted Sup-region TCAM Entries**

This example shows how to perform an on-demand detection of corrupted sup-region TCAM entries:

```
hardware sup-tcam monitoring trigger-detection
```

**Configuring Periodic Detection of Corrupted Sup-region TCAM Entries**

This example shows how to configure periodic detection of corrupted sup-region TCAM entries:

```
configure terminal
  hardware sup-tcam monitoring enable
  hardware sup-tcam monitoring timer-expiry 1500
```

**Correcting the Corrupted Sup-region TCAM Entries**

This example shows how to correct the corrupted sup-region TCAM entries:

```
hardware sup-tcam correction asic 2 entry 2172
```

Additional References for Sup-region TCAM Monitoring

This section describes additional information related to implementing Sup-region TCAM Monitoring.

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS licensing</td>
<td><em>Cisco NX-OS Licensing Guide</em></td>
</tr>
<tr>
<td>Command reference</td>
<td></td>
</tr>
</tbody>
</table>
Feature History for Sup-region TCAM Monitoring

This table lists the release history for this feature.

*Table 21: Feature History for Sup-region TCAM Monitoring*

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sup-region TCAM Monitoring</td>
<td>Cisco NX-OS Release 7.1(4)N1(1)</td>
<td>The Sup-region Ternary Content-Addressable Memory (TCAM) Monitoring feature is a monitoring mechanism that enables detection, reporting and correction of sup-region TCAM entry corruption.</td>
</tr>
</tbody>
</table>
INDEX

802.1X  73, 76, 77, 79, 80, 81, 82, 83, 84, 85, 88, 92, 93, 94, 95, 96, 98, 100, 101
authenticator PAEs  76
configuration process  82
configuring  82
configuring AAA accounting methods  98
configuring AAA authentication methods  83
configuring on member ports  85
controlling on interfaces  84
default settings  81
description  73
disabling authentication  94
disabling feature  95
enabling feature  82
enabling MAC authentication bypass  93
enabling multiple hosts mode  92
enabling periodic reauthentication on interfaces  88
enabling single host mode  92
example configuration  101
guidelines  80
licensing requirements  80
limitations  80
MAC authentication bypass  77
monitoring  101
multiple host support  79
prerequisites  80
setting interface maximum retransmission retry count  96
single host support  79
supported topologies  79
verifying configuration  100
802.1X authentication  75, 76, 90, 97
authorization states for ports  76
changing timers on interfaces  90
enabling RADIUS accounting initiation  75
manually initializing  90
802.1X reauthentication  99
setting maximum retry count on interfaces  99
802.1X supplicants  89
manually reauthenticating  89

AAA  3, 5, 6, 7, 9, 10, 12, 13, 40, 83, 115, 116, 118
accounting  5
AAA (continued)
authentication  5
benefits  6
configuring authentication methods for 802.1X  83
Configuring Console Authorization Commands  12
configuring console login  10
configuring for Cisco TrustSec  115
configuring for RADIUS servers  40
configuring nonseed device for Cisco TrustSec  118
configuring seed device for Cisco TrustSec  116
default settings  9
description  3
enabling MSCHAP authentication  13
guidelines  9
limitations  9
prerequisites  9
user login process  7
AAA accounting  14, 98
configuring default methods  14
configuring methods for 802.1X  98
AAA accounting logs  27
clearing  27
displaying  27
AAA logins  12
AAA protocols  5
RADIUS  5
TACACS+  5
AAA server groups  6
description  6
AAA servers  14, 16
specifying SNMPv3 parameters  14, 16
specifying user roles  16
specifying user roles in VSAs  14
AAA services  6
configuration options  6
remote  6
accounting  5
description  5
ACL  150, 152
processing order  150
sequence numbers  152
ACL implicit rules  151
ACLs  143, 151, 155, 156, 159, 172
applications  149
### ACLs (continued)
- creating log entries for guidelines
- identifying traffic by protocols
- licensing
- limitations
- prerequisites
- types VLAN
- authentication 802.1X Cisco TrustSec configuring for Cisco TrustSec description 5
- local methods
- remote methods
- user login authentication
- authenticator PAEs creating on an interface description removing from an interface authorization user login

###Cisco
- Cisco vendor ID
- Cisco TrustSec architecture
- authorization
- configuring
- configuring AAA on nonseed device
- configuring AAA on seed device
- configuring device credentials
- default values
- description
- enabling
- enabling (example)
- environment data download
- example configurations
- guidelines
- licensing
- limitations
- manually configuring SXP
- policy acquisition
- prerequisites
- RADIUS relay
- SGACLs
- SGTs
- verifying configuration
- Cisco TrustSec authentication 802.1X role selection description
- configuration process

###Cisco TrustSec authentication (continued)
- configuring EAP-FAST enhancements
- manual mode configuration examples
- summary
- Cisco TrustSec authorization
- configuration process
- configuring
- Cisco TrustSec device credentials
- description
- Cisco TrustSec device identities
- description
- Cisco TrustSec environment data download
- Cisco TrustSec policies example enforcement configuration
- Cisco TrustSec seed devices
- configuration process
- configuring
- Cisco TrustSec device identities
- description
- example configuration
- Cisco TrustSec user credentials
- description
cisco-av-pair specifying AAA user parameters
- class maps
- CoPP
- clearing statistics
- CoPP
- committing
- user defined template
- configuration status
- CoPP
- control plane policies
- applying
- control plane class maps
- verifying the configuration
- control plane policy maps
- verifying the configuration
- control plane protection
- CoPP
- packet types
- control plane protection, classification
- control plane protection, CoPP
- rate controlling mechanisms
- CoPP
class maps
- clearing statistics
- configuration status
- control plane protection
- control plane protection, classification
- default settings
- guidelines
- information about licensing
CoPP (continued)
  limitations 239
  monitoring 244
  policy templates 234
  restrictions for management interfaces 239
  verifying the configuration 243
CoPP policies 234, 236, 237, 238, 241
  applying 241
  customized 238
  default 234
  scaled Layer 2 236
  scaled Layer 3 237
CoPP policy 241
  customized 241
  modifying 241
creating 250
user defined template 250
CTS, See Cisco TrustSec
customized CoPP policy 238, 241
  modifying 241

D
default settings 187
  port security 187
default CoPP policy 234
default settings 9, 81, 240
  802.1X 81
  AAA 9
  CoPP 240
device roles 73
  description for 802.1X 73
DHCP binding database 203
DHCP Option 82 203
  description 203
DHCP relay agent 206, 214, 215, 216, 217
  described 206
  enabling or disabling 214
  enabling or disabling Option 82 215
  enabling or disabling subnet broadcast support on a Layer 3 Interface 217
  enabling or disabling VRF support 216
  VRF support 206
DHCP relay binding database 207
  description 207
DHCP relay statistics 226
  clearing 226
DHCP snooping 201, 203, 205, 208
  binding database 203
  default settings 208
  description 201
  guidelines 208
  in a vPC environment 205
  limitations 208
  message exchange process 203
  Option 82 203
DHCP snooping (continued)
  overview 201
DHCP snooping binding database 203
  described 203
  description 203
  entries 203
DHCPv6 relay 221
  configuring the source interface 221
DHCPv6 relay agent 207, 219, 220
  described 207
  enabling or disabling 219
  enabling or disabling VRF support 220
  VRF support 207
DHCPv6 relay statistics 226
  clearing 226
Dynamic Host Configuration Protocol snooping. See DHCP snooping

E
eamples 28
  AAA configurations 28

G
guidelines 156, 186, 208, 239
  ACLs 156
  CoPP 239
  DHCP snooping 208
  port security 186

I
IDs 15, 31
  Cisco vendor ID 15, 31
  information about 247
  default template 247
  user-defined templates 247
IP ACL implicit rules 151
IP ACLs 4, 149, 153, 158, 159, 161, 162
  applications 149
  applying as a Router ACL 161
  applying as port ACLs 162
  changing 158
  changing sequence numbers in 159
  description 4
  logical operation units 153
  logical operators 153
  removing 159
  types 149

L
LDRA 207
  described 207
INDEX

P

policy templates 234
description 234
policy-based ACLs 153, 168
description 153
verifying object groups 168
port ACL 162
port security 181, 184, 186, 187
default settings 187
guidelines 186
limitations 186
MAC address learning 181
MAC move 184
violations 184
ports 76
authorization states for 802.1X 76
preshared keys 48
TACACS+ 48

R

RADIUS 4, 29, 30, 32, 38, 44, 45, 111
counting servers 32
counting timeout intervals 38
counting transmission retry counts 38
default settings 32
description 4
deleteatures 45
example configurations 45
monitoring 30
network environments 29
operations 30
prerequisites 32
relay for Cisco TrustSec 111
statistics, displaying 44
RADIUS accounting 97
counting for 802.1X authentication 97
RADIUS server groups 37
global source interfaces 37
RADIUS server preshared keys 35
RADIUS servers 38, 39, 40, 42, 43, 45
allowing users to specify at login 38
counting AAA for 40
counting timeout interval 39
counting transmission retry count 39
deleting hosts 42
disable example configurations 45
manually monitoring 43
RADIUS statistics 44
clearing 44
RADIUS, global preshared keys 34
RADIUS, periodic server monitoring 41
RADIUS, server hosts 33
counting 33
rate controlling mechanisms 231
control plane protection, CoPP 231

M

MAC ACL implicit rules 151
MAC ACLs 168
ACLs 168
MAC 168
creating 168
creating 168
MAC addresses 181
learning 181
MAC authentication 77, 93
bypass for 802.1X 77
enabling bypass in 802.1X 93
management interfaces 239
CoPP restrictions 239
modifying 251
user defined template 251
monitoring 30, 41, 244
CoPP 244
RADIUS 30
RADIUS servers 41
MSCHAP 13
enabling authentication 13

O

object groups 153, 164, 168
configuring 164
description 153
verifying 168

licensing 80, 112, 155, 239, 256
802.1X 80
ACLs 155
Cisco TrustSec 112
CoPP 239
Lightweight DHCPv6 relay agent 207, 208
described 207
guidelines and limitations 208
limitations 156, 186, 208, 239
ACLs 156
CoPP 239
DHCP snooping 208
port security 186
logging 159
creating ACL for 159
logical operation units 153
IP ACLs 153
logical operators 153
IP ACLs 153
login 38
RADIUS servers 38
LOU, See logical operation units
remote devices 68
  connecting to using SSH 68
router ACLs 161
rules 151
  implicit 151

S
  scaled Layer 2 CoPP policy 236
  scaled Layer 3 CoPP policy 237
secure MAC addresses 181
  learning 181
security 181, 241
  policies 241
    applying 241
    port 181
    MAC address learning 181
  security group access lists, See SGACLs
  security group tag, See SGT
server groups 6
  servers 38
    RADIUS 38
SGACL policies 132, 134, 135
  clearing 135
  displaying downloaded policies 134
  manually configuring 132
SGACL policy enforcement 127, 128
  enabling on VLANs 127
  enabling on VRF instances 128
SGACLs 107, 126, 145
  configuring 126
  description 107
  example manual configuration 145
  example SGT mapping configuration 145
SGACLs policies 110, 135
  acquisition 110
  refreshing downloaded policies 135
SGTs 107, 109, 129, 130, 131, 145
  description 107
  example mapping configuration 145
  manually configuring 129
  manually configuring address-to-SGACL mapping 130, 131
  propagation with SXP 109
SNMPv3 14, 16
  specifying AAA parameters 14
  specifying parameters for AAA servers 16
source interfaces 37, 55
  RADIUS server groups 37
  TACACS+ server groups 55
SSH 4
  description 4
SSH clients 63
SSH server keys 63
SSH servers 63
  SSH sessions 68, 69
    clearing 69
    connecting to remote devices 68
statistics 60
  TACACS+ 60
SXP 109, 136, 137, 139, 140, 141
  changing reconcile periods 141
  changing retry periods 141
  configuration process 136
  configuring default passwords 139
  configuring default source IP addresses 140
  configuring manually 136
  configuring peer connections 137
  enabling 136
  SGT propagation 109
SXP connections 146
  example manual configuration 146
T
  TACACS+ 4, 47, 48, 49, 50, 56, 60, 61
    advantages over RADIUS 47
    configuring 50
    configuring global timeout interval 56
    description 4, 47
    displaying statistics 60
    example configurations 61
    field descriptions 50
    global preshared keys 48
    limitations 50
    prerequisites 49
    preshared key 48
    user login operation 48
  TACACS+ server groups 55
    global source interfaces 55
  TACACS+ servers 50, 51, 56, 57, 60
    configuring hosts 51
    configuring TCP ports 57
    configuring timeout interval 56
    field descriptions 50
    manually monitoring 60
  TCP ports 57
    TACACS+ servers 57
Telnet 4
  description 4
Telnet server 71
  enabling 71
  reenabling 71
Telnet servers 64
Telnet sessions 71, 72
  clearing 72
  connecting to remote devices 71
INDEX

U

user defined template 250, 251
  committing 251
  creating 250
  modifying 251
user login 7
  authentication process 7
  authorization process 7
user roles 14, 16
  specifying on AAA servers 14, 16
user-defined templates 247
  information about 247

V

vendor-specific attributes 15
verifying 28, 44, 61, 253
  AAA configuration 28
  RADUIS configuration 44
  TACACS+ configuration 61
  TCAM carving configuration 253
VLAN ACLs 172
  information about 172
vPCs 205
  and DHCP snooping 205
VSAs 15, 16
  format 16
  protocol options 16
  support description 15