Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x

First Published: 2012-07-27

Last Modified: 2019-11-05

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

Text Part Number: OL-25776-03

CONTENTS

Preface

The preface contains the following sections:

Audience

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

Document Conventions

Note 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:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.

Convention	Description
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

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

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.

Related Documentation for Cisco Nexus 7000 Series NX-OS Software

The entire Cisco Nexus 7000 Series NX-OS documentation set is available at the following URL:

https://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/series.html#~tab-documents

Release Notes

The release notes are available at the following URL:

http://www.cisco.com/en/US/products/ps9402/prod_release_notes_list.html

Configuration Guides

These guides are available at the following URL:

http://www.cisco.com/en/US/products/ps9402/products_installation_and_configuration_guides_list.html

The documents in this category include:

- *Cisco Nexus 7000 Series NX-OS Configuration Examples*
- *Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS IP SLAs Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS LISP Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS OTV Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS SAN Switching Guide*
- *Cisco Nexus 7000 Series NX-OS Security Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*
- *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start*
- *Cisco Nexus 7000 Series NX-OS OTV Quick Start Guide*
- *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*
- *Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*

Command References

These guides are available at the following URL:

http://www.cisco.com/en/US/products/ps9402/prod_command_reference_list.html

The documents in this category include:

- *Cisco Nexus 7000 Series NX-OS Command Reference Master Index*
- *Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*
- *Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference*
- *Cisco Nexus 7000 Series NX-OS High Availability Command Reference*
- *Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*
- *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*
- *Cisco Nexus 7000 Series NX-OS LISP Command Reference*
- *Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*
- *Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*
- *Cisco Nexus 7000 Series NX-OS OTV Command Reference*
- *Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*
- *Cisco Nexus 7000 Series NX-OS SAN Switching Command Reference*
- *Cisco Nexus 7000 Series NX-OS Security Command Reference*
- *Cisco Nexus 7000 Series NX-OS System Management Command Reference*
- *Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference*
- *Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference*
- *Cisco NX-OS FCoE Command Reference for Cisco Nexus 7000 and Cisco MDS 9500*

Other Software Documents

You can locate these documents starting at the following landing page:

https://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/series.html#~tab-documents

- *Cisco Nexus 7000 Series NX-OS MIB Quick Reference*
- *Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide*
- *Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*
- *Cisco NX-OS Licensing Guide*
- *Cisco NX-OS System Messages Reference*
- *Cisco NX-OS Interface User Guide*

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.
- 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.

CHAPTER 1

New and Changed Information

New and Changed Information

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 1: New and Changed Security Features

Feature	Description	Changed in Release	Where Documented
Control Plane Policing	Added the functionality to classify and rate-limit IP unicast RPF failure packets.	6.2(10)	Configuring Control Plane Policing, on page 619
ACL TCAM bank mapping	Added a command to display the bank mapping matrix.	6.2(10)	Configuring IP ACLs, on page 405
Cisco TrustSec	Added SGT support for F3 Series modules.	6.2(10)	Configuring Cisco TrustSec
DHCP relay trusted interfaces	Added support for the following commands: • **ip dhcp relay information option trust** • **ip dhcp relay information trusted** • **ip dhcp relay information trust-all**	6.2(8)	Configuring DHCP, on page 509
Cisco TrustSec	Enabled MACSec support for F2e modules. Added support for batching SGACL programming tasks.	6.2(6)	Configuring Cisco TrustSec
Cisco TrustSec	Added the ability to map VLANs to SGTs.	6.2(2)	Configuring Cisco TrustSec

Feature	Description	Changed in Release	Where Documented
Cisco TrustSec	Added the ability to encrypt the SAP PMK and display the PMK in encrypted format in the running configuration.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Added the **show cts sap pmk** command to display the hexadecimal value of the configured PMK.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Added the **show cts capability interface** command to display the Cisco TrustSec capability of interfaces.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Enabled the **cts sgt**, **policy static sgt**, and **clear cts policy sqt** commands to accept decimal values.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Added the ability to download sgname tables from ISE and to refresh the environment data manually and upon environment data timer expiry.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Added optional keywords to the **show cts role-based sgt-map** command to display a summary of the SGT mappings or the SGT map configuration for a specific SXP peer, VLAN, or VRF.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Added the **brief** keyword to the **show cts interface** command to display a brief summary for all CTS-enabled interfaces.	6.2(2)	Configuring Cisco TrustSec
Cisco TrustSec	Added SGT support for F2 and F2e Series modules.	6.2(2)	Configuring Cisco TrustSec
CoPP	Updated the output of the **show policy-map interface control-plane** command to show the 5-minute moving averages and peaks of the conformed and violated byte counts for each policy in each module.	6.2(2)	Configuring Control Plane Policing, on page 619
CoPP	Added VRRP6 ACL support to police VRRP IPv6 traffic. The HSRP ACL is modified to reflect the correct destination addresses of control packets.	6.2(2)	Configuring Control Plane Policing, on page 619
CoPP	Changed the behavior of multicast traffic from being policed at different rates in different classes to being grouped into three classes (multicast-host, multicast-router, and normal) and policed at consistent rates.	6.2(2)	Configuring Control Plane Policing, on page 619

Feature	Description	Changed in Release	Where Documented
CoPP	Added the ability to monitor CoPP with SNMP.	6.2(2)	Configuring Control Plane Policing, on page 619
DHCP	Added support for the DHCPv6 relay agent.	6.2(2)	Configuring DHCP, on page 509
IP ACLs	Added support for ACL TCAM bank mapping.	6.2(2)	Configuring IP ACLs, on page 405
IP ACLs	Added support for ACL TCAM bank mapping.	6.2(2)	Configuring IP ACLs, on page 405
Rate limits	Added support for Layer 3 glean fast-path packets.	6.2(2)	Configuring Rate Limits, on page 665
VLAN ACLs	Added support for deny ACEs in a sequence.	6.1(3)	Configuring VLAN ACLs, on page 473
Cisco TrustSec	Removed the requirement for the Advanced Services license.	6.1(1)	Configuring Cisco TrustSec
Cisco TrustSec	Added MACsec support for 40G and 100G M2 Series modules.	6.1(1)	Configuring Cisco TrustSec
CoPP	Added a new class for FCoE; added the LISP, LISP6, and MAC Layer 3 IS-IS ACLs to the critical class; added the fcoe-fib-miss match exception to the undesirable class; added the MAC Layer 2 tunnel ACL to the Layer 2 unpoliced class, and added the "permit icmp any any 143" rule to the acl-icmp6-msgs ACL.	6.1(1)	Configuring Control Plane Policing, on page 619
FIPS	Added support for digital image signing on switches that contain the Supervisor 2 module.	6.1(1)	Configuring FIPS, on page 17
FIPS	Updated FIPS guidelines for M2 Series modules.	6.1(1)	Configuring FIPS, on page 17
IP ACLs and MAC ACLs	Updated for M2 Series modules.	6.1(1)	Configuring IP ACLs, on page 405 and Configuring MAC ACLs, on page 461
Cisco TrustSec	Updated for F2 Series modules.	6.0(1)	Configuring Cisco TrustSec
CoPP	Added the dense default CoPP policy.	6.0(1)	Configuring Control Plane Policing, on page 619

Feature	Description	Changed in Release	Where Documented
CoPP	Added the ability to configure the CoPP scale factor per line card.	6.0(1)	Configuring Control Plane Policing, on page 619
FIPS	Updated FIPS guidelines for F2 Series modules.	6.0(1)	Configuring FIPS, on page 17
IP ACLs, MAC ACLs, and VACLs	Updated for F2 Series modules.	6.0(1)	Configuring IP ACLs, on page 405, Configuring MAC ACLs, on page 461, and Configuring VLAN ACLs, on page 473
Rate limits	Added support for F2 Series modules.	6.0(1)	Configuring Rate Limits, on page 665
RBAC	Added support for F2 Series modules.	6.0(1)	Configuring User Accounts and RBAC, on page 235
TACACS+	Added the ability to configure command authorization for a console session.	6.0(1)	Configuring TACACS+, on page 93
User accounts and RBAC	Added the ability to configure a read-only or read-and-write rule for an SNMP OID.	6.0(1)	Configuring User Accounts and RBAC, on page 235
ACLs and CoPP	Changed the **show running-config aclmgr** and **show startup-config aclmgr** commands to display only the user-configured ACLs (and not also the default CoPP-configured ACLs) in the running and startup configurations.	5.2(1)	Configuring IP ACLs, on page 405, Configuring MAC ACLs, on page 461, Configuring VLAN ACLs, on page 473, and Configuring Control Plane Policing, on page 619
Cisco TrustSec	Added support for pause frame encryption and decryption on interfaces.	5.2(1)	Configuring Cisco TrustSec
CoPP	Added the ability to change or reapply the default CoPP policy without rerunning the setup utility.	5.2(1)	Configuring Control Plane Policing, on page 619
CoPP	Changed the CoPP best practice policy to read-only and added the ability to copy the policy in order to modify it.	5.2(1)	Configuring Control Plane Policing, on page 619

Feature	Description	Changed in Release	Where Documented
CoPP	Added the **show copp profile** and **show copp diff profile** commands to display the details of the CoPP best practice policy and the differences between policies, respectively.	5.2(1)	Configuring Control Plane Policing, on page 619
CoPP	Changed the **show copp status** command to display which flavor of the CoPP best practice policy is attached to the control plane.	5.2(1)	Configuring Control Plane Policing, on page 619
CoPP	Changed the name of the **none** option for the best practices CoPP profile in the setup utility to **skip**.	5.2(1)	Configuring Control Plane Policing, on page 619
CoPP	Updated the default class maps with support for MPLS LDP, MPLS OAM, MPLS RSVP, DHCP relay, and OTV-AS.	5.2(1)	Configuring Control Plane Policing, on page 619
DHCP	Added subnet broadcast support for the DHCP relay agent and support for DHCP smart relay.	5.2(1)	Configuring DHCP, on page 509
FCoE ACLs	Added support for FCoE ACLs on F1 Series modules.	5.2(1)	Configuring IP ACLs, on page 405
IP ACLs	Added support for ACL capture on M1 Series modules.	5.2(1)	Configuring IP ACLs, on page 405
LDAP	Deprecated the **ldap-server port** command.	5.2(1)	Configuring LDAP, on page 137
Password encryption	Added support for AES password encryption and a configurable master encryption key.	5.2(1)	Configuring Password Encryption, on page 583
RADIUS	Added type-6 encryption support for RADIUS server keys.	5.2(1)	Configuring RADIUS, on page 61
TACACS+	Added type-6 encryption support for TACACS+ server keys.	5.2(1)	Configuring TACACS+, on page 93
Control plane policy map	Added the ability to specify the threshold value for dropped packets and generate a syslog if the drop count exceeds the configured threshold.	5.1(1)	Configuring Control Plane Policing, on page 619
CoPP	Updated the default policies with the 802.1Q class of service (cos) values.	5.1(1)	Configuring Control Plane Policing, on page 619
CoPP	Added support for non-IP traffic classes.	5.1(1)	Configuring Control Plane Policing, on page 619

Feature	Description	Changed in Release	Where Documented
DHCP snooping	Optimized DHCP snooping to work in a vPC environment.	5.1(1)	Configuring DHCP, on page 509
FIPS	Added the ability to configure Federal Information Processing Standards (FIPS) mode.	5.1(1)	Configuring FIPS, on page 17
Rate limits	Added support for F1 Series module packets.	5.1(1)	Configuring Rate Limits, on page 665
Rate limits	Added the ability to configure rate limits for packets that reach the supervisor module and to log a system message if the rate limit is exceeded.	5.1(1)	Configuring Rate Limits, on page 665
Rate limits	Added options to disable rate limits and to configure rate limits for a specific module and port range.	5.1(1)	Configuring Rate Limits, on page 665
SCP and SFTP servers	Added the ability to configure SCP and SFTP servers on the Cisco NX-OS device to support the copy of files to and from a remote device.	5.1(1)	Configuring SSH and Telnet, on page 163
User roles	Added the ability to display the syntax of the commands that the network-admin and network-operator roles can use.	5.1(1)	Configuring User Accounts and RBAC, on page 235
VTY ACLs	Added support to control access to traffic received over a VTY line.	5.1(1)	Configuring IP ACLs, on page 405
802.1X	Supports configuring 802.1X on member ports of a port channel.	5.0(2)	Configuring 802.1X, on page 263
AAA authorization	Supports configuring the default AAA authorization method for TACACS+ servers.	5.0(2)	Configuring TACACS+, on page 93
CHAP authentication	Allows the enabling or disabling of CHAP authentication.	5.0(2)	Configuring AAA, on page 25
CoPP	Updated the default policies with support for ACL HSRP6.	5.0(2)	Configuring Control Plane Policing, on page 619
DHCP	Allows the DHCP relay agent to support VRFs. Also adds the **ip dhcp relay information option vpn** command and modifies the **ip dhcp relay address** command.	5.0(2)	Configuring DHCP, on page 509

Feature	Description	Changed in Release	Where Documented
DHCP	Supports enabling DHCP to use Cisco proprietary numbers 150, 152, and 151 for the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.	5.0(2)	Configuring DHCP, on page 509
IP ACLs, MAC ACLs, and VACLs	Allows up to 128K ACL entries when using an XL line card, provided a scalable services license is installed.	5.0(2)	Configuring IP ACLs, on page 405, Configuring MAC ACLs, on page 461, and Configuring VLAN ACLs, on page 473
LDAP	Supports configuring the Lightweight Directory Access Protocol (LDAP).	5.0(2)	Configuring LDAP, on page 137
Local authentication	Enables fallback to local authentication when remote authentication fails.	5.0(2)	Configuring AAA, on page 25
Local authentication	Allows the disabling of fallback to local authentication.	5.0(2)	Configuring AAA, on page 25
OTP	Supports one-time passwords.	5.0(2)	Configuring RADIUS, on page 61
Periodic server monitoring	Supports global periodic RADIUS and TACACS+ server monitoring.	5.0(2)	Configuring RADIUS, on page 61 and Configuring TACACS+, on page 93
PKI	Supports a remote cert-store and certificate mapping filters.	5.0(2)	Configuring PKI, on page 187
Privilege roles	Supports permitting or denying commands for users of privilege roles.	5.0(2)	Configuring TACACS+, on page 93
Rate limits	Supports Layer 2 Tunnel Protocol (L2TP) packets.	5.0(2)	Configuring Rate Limits, on page 665
SGACL policies	Allows the enabling or disabling of RBACL logging.	5.0(2)	Configuring Cisco TrustSec, on page 341
SGACL policies	Allows the enabling, disabling, monitoring, and clearing of RBACL statistics.	5.0(2)	Configuring Cisco TrustSec, on page 341
SSH	Supports configuring a maximum number of SSH login attempts.	5.0(2)	Configuring SSH and Telnet, on page 163

Feature	Description	Changed in Release	Where Documented
SSH	Supports starting SSH sessions from the boot mode of a Cisco NX-OS device in order to connect to a remote device.	5.0(2)	Configuring SSH and Telnet, on page 163
SSH	Supports copying files from a Cisco NX-OS device to an SCP or SFTP server without a password.	5.0(2)	Configuring SSH and Telnet, on page 163
TACACS+ privilege-level authorization	Supports the mapping of privilege levels configured for users on the TACACS+ server to locally configured user roles on the Cisco NX-OS device.	5.0(2)	Configuring TACACS+, on page 93

CHAPTER 2

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.

This chapter includes the following sections:

Licensing Requirements

For a complete explanation of Cisco NX-OS licensing recommendations and how to obtain and apply licenses, see the *Cisco NX-OS Licensing Guide*.

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.

Note 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.

LDAP

The Lightweight Directory Access Protocol (LDAP) provides centralized validation of users attempting to gain access to a Cisco NX-OS device. LDAP allows a single access control server (the LDAP daemon) to provide authentication and authorization independently.

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.

PKI

The Public Key Infrastructure (PKI) allows the device to obtain and use digital certificates for secure communication in the network and provides manageability and scalability for applications, such as SSH, that support digital certificates.

User Accounts and Roles

You can create and manage user accounts and assign roles that limit access to operations on the Cisco NX-OS device. Role-based access control (RBAC) allows you to define the rules for an assign role that restrict the authorization that the user has to access management operations.

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 an 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.

NAC

Network Admission Control (NAC) allows you to check endpoint devices for security compliancy and vulnerability before these devices are allowed access to the network. This security compliancy check is referred to as *posture validation*. Posture validation allows you to prevent the spread of worms, viruses, and other rogue applications across the network.

NAC validates that the posture, or state, of endpoint devices complies with security policies before the devices can access protected areas of the network. For devices that comply with the security policies, NAC allows access to protected services in the network. For devices that do not comply with security policies, NAC restricts access to the network that is sufficient only for remediation, which checks the posture of the device again.

Cisco TrustSec

The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices. Each device in the cloud is authenticated by its neighbors. Communication on the links between devices in the cloud is secured with a combination of encryption, message integrity checks, and replay protection mechanisms. Cisco TrustSec also uses the device and user identification 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. Cisco TrustSec uses ingress tagging and egress filtering to enforce access control policy in as a conversation.

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.

MAC ACLs

MAC ACLs are ACLs that filter traffic using the information in the Layer 2 header of each packet. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When the Cisco NX-OS software determines that a MAC 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 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.

VACLs

A VLAN ACL (VACL) is one application of an IP ACL or MAC ACL. You can configure VACLs to apply to all packets that are routed into or out of a VLAN or are bridged within a VLAN. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VACLs are not defined by direction (ingress or egress).

Port Security

Port security allows you to configure Layer 2 interfaces that 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.

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.

Dynamic ARP inspection (DAI) and IP Source Guard also use information stored in the DHCP snooping binding database.

Dynamic ARP Inspection

Dynamic ARP inspection (DAI) ensures that only valid ARP requests and responses are relayed. When DAI is enabled and properly configured, a Cisco NX-OS device performs these activities:

- Intercepts all ARP requests and responses on untrusted ports.
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination.
- Drops invalid ARP packets.

DAI can determine the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the device. If the ARP packet is received on a trusted interface, the device forwards the packet without any checks. On untrusted interfaces, the device forwards the packet only if it is valid.

IP Source Guard

IP Source Guard is a per-interface traffic filter that permits IP traffic only when the IP address and MAC address of each packet matches one of two sources of IP and MAC address bindings:

- Entries in the DHCP snooping binding table.
- Static IP source entries that you configure.

Filtering on trusted IP and MAC address bindings helps prevent attacks that rely on spoofing the IP address of a valid host. To circumvent IP Source Guard, an attacker would have to spoof both the IP address and the MAC address of a valid host.

Password Encryption

The Advanced Encryption Standard (AES) password encryption feature stores all existing and newly created clear-text passwords for supported applications (currently RADIUS and TACACS+) in the strong and reversible type-6 encrypted format. A master encryption key is used to encrypt and decrypt the passwords. You can also use this feature to convert all existing weakly encrypted passwords to type-6 encrypted passwords.

Keychain Management

Keychain management allows you to create and maintain keychains, which are sequences of keys (sometimes called shared secrets). You can use keychains with features that secure communications with other devices by using key-based authentication. The device allows you to configure multiple keychains.

Some routing protocols that support key-based authentication can use a keychain to implement a hitless key rollover for authentication.

Unicast RPF

The Unicast Reverse Path Forwarding (RPF) feature reduces problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of Denial-of-Service (DoS) attacks, including Smurf and Tribal Flood Network (TFN) attacks, can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. Unicast RPF deflects attacks by forwarding only the packets that have source addresses that are valid and consistent with the IP routing table.

Traffic Storm Control

Traffic storm control (also called traffic suppression) allows you to monitor the levels of the incoming traffic over a 1-second interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.

Control Plane Policing

The Cisco NX-OS device provides control plane policing to prevent denial-of-service (DoS) attacks from impacting performance. The supervisor module of the Cisco NX-OS device has both the management plane and control plane and is critical to the operation of the network. Any disruption to the supervisor module would result in serious network outages. Excessive traffic to the supervisor module could overload it and slow down the performance of the entire Cisco NX-OS device. Attacks on the supervisor module can be of various types such as, denial-of-service (DoS) attacks that generate IP traffic streams to the control plane at a very high rate. These attacks result in the control plane spending a large amount of time in handling these packets, which makes the control plane unable to process genuine traffic.

Rate Limits

Rate limits can prevent redirected packets for egress exceptions from overwhelming the supervisor module on a Cisco NX-OS device.

CHAPTER 3

Configuring FIPS

This chapter describes how to configure the Federal Information Processing Standards (FIPS) mode on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About FIPS

The FIPS 140-2 Publication, *Security Requirements for Cryptographic Modules*, details the U.S. government requirements for cryptographic modules. FIPS 140-2 specifies that a cryptographic module shall be a set of hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary.

FIPS specifies certain cryptographic algorithms as secure, and it identifies which algorithms should be used if a cryptographic module is to be called FIPS compliant.

FIPS Self-Tests

A cryptographic module must perform power-up self-tests and conditional self-tests to ensure that it is functioning properly.

Power-up self-tests run automatically after the device powers up. A device goes into FIPS mode only after all self-tests are successfully completed. If any self-test fails, the device logs a system message and moves into an error state.

The device uses a cryptographic algorithm known-answer test (KAT) to test FIPS mode for each FIPS 140-2-approved cryptographic function (encryption, decryption, authentication, and random number generation) implemented on the device. The device applies the algorithm to data for which the correct output is already known. It then compares the calculated output to the previously generated output. If the calculated output does not equal the known answer, the KAT fails.

Conditional self-tests run automatically when an applicable security function or operation is invoked. Unlike the power-up self-tests, conditional self-tests are executed each time their associated function is accessed.

Conditional self-tests include the following:

Pair-wise consistency test

This test is run when a public or private key-pair is generated.

Continuous random number generator test

This test is run when a random number is generated.

The Cisco TrustSec manager also runs a bypass test to ensure that encrypted text is never sent as plain text.

Note A bypass test failure on CTS-enabled ports causes only those corresponding ports to be shut down. The bypass test might fail because of packet drops caused by data path congestion. In such cases, we recommend that you try bringing up the port again.

FIPS Error State

When the system is booted up in FIPS mode, the FIPS power-up self-tests run on the supervisor and line card modules. If any of these bootup tests fail, the whole system is moved to the FIPS error state. In this state, as per the FIPS requirement, all cryptographic keys are deleted, and all line cards are shut down. This mode is exclusively meant for debugging purposes.

Once the switch is in the FIPS error state, any reload of a line card moves it to the failure state. To move the switch back to FIPS mode, it has to be rebooted. However, once the switch is in FIPS mode, any power-up self-test failure on a subsequent line card reload or insertion affects only that line card, and only the corresponding line card is moved to the failure state.

RADIUS Keywrap

RADIUS keywrap support is an extension of the RADIUS protocol. It provides a FIPS-certifiable means for the Cisco Access Control Server (ACS) to authenticate RADIUS messages and distribute session keys.

RADIUS keywrap increases RADIUS protocol security by using the Advanced Encryption Standard (AES) keywrap algorithm to transfer keys while an HMAC-SHA1 algorithm is used to protect packet integrity. It specifies that the key encryption key (KEK) and the hash key must be different from each other, should not be based on a password, and must be cryptographically independent of the RADIUS shared secret used in calculating the response authenticator.

Note The proxy and message authenticator are not supported for RADIUS keywrap.

When FIPS mode is enabled, RADIUS keywrap is enabled automatically. As a result, keywrap attributes are added to any RADIUS request that contains EAP attributes but is not meant for protected access credential (PAC) provisioning. The attributes are sent to the Cisco ACS, which distributes the EAP-TLS session key to an IEEE 802.1X EAP authenticator. The session key is encrypted using AES, and the RADIUS message is authenticated using HMAC-SHA-1.

Note Cisco ACS Release 5.2 supports the RADIUS keywrap feature.

Virtualization Support for FIPS

You can configure FIPS mode and run FIPS self-tests only in the default virtual device context (VDC). For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Prerequisites for FIPS

FIPS has the following prerequisites:

- Disable Telnet. Users should log in using Secure Shell (SSH) only.
- Disable SNMPv1 and v2. Any existing user accounts on the device that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy.
- Delete all SSH server RSA1 key-pairs.
- Enable HMAC-SHA1 message integrity checking (MIC) for use during the Cisco TrustSec Security Association Protocol (SAP) negotiation. To do so, enter the **sap hash-algorithm HMAC-SHA-1** command from the cts-manual or cts-dot1x mode. Note that this command is not supported for F1 Series or F2 Series modules.

Guidelines and Limitations for FIPS

FIPS has the following configuration guidelines and limitations:

- The RADIUS keywrap feature works only with Cisco ACS Release 5.2 or later releases.
- The user authentication mechanisms supported for SSH are usernames and passwords, public keys, and X.509 certificates.
- Your passwords should have a minimum of eight alphanumeric characters.

- The F1 Series and F2 Series modules do not support FIPS mode. However, you can deploy an F1 Series or F2 Series module in a Cisco NX-OS device that is operating in FIPS mode.
- The F1 Series and F2 Series modules do not support the cts-dot1x mode or the cts-manual mode.
- Digital image signing is supported on Cisco Nexus 7000 Series switches that contain the Supervisor 2 module.
- The M2 Series modules do not support FIPS mode. However, you can deploy an M2 Series module in a Cisco NX-OS device that is operating in FIPS mode.

Default Settings for FIPS

This table lists the default settings for FIPS parameters.

Table 2: Default FIPS Parameters

Parameters	Default
FIPS mode	Disabled

Configuring FIPS

This section describes how to configure FIPS mode on Cisco NX-OS devices.

Enabling FIPS Mode

Beginning with Cisco NX-OS Release 5.1, you can enable FIPS mode on the device.

Before you begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. **configure terminal**
2. **fips mode enable**
3. **exit**
4. (Optional) **show fips status**
5. **copy running-config startup-config**
6. **reload**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**fips mode enable** **Example:** `switch(config)# fips mode enable`	Enables FIPS mode. **Note** **fips mode enable** could be typed only when All LC s are online or else it leads to LC failure.

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

Step 4	(Optional) **show fips status**
	Example:
	`switch# show fips status`
	`FIPS mode is enabled`
		Displays the status of FIPS mode.

Step 5	Required: **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.
Step 6	Required: **reload** **Example:** `switch# reload`	Reloads the Cisco NX-OS device. **Note** After you enable FIPS, a reboot is required for the system to operate in FIPS mode.

Related Topics

Disabling FIPS Mode, on page 21

Disabling FIPS Mode

You can disable FIPS mode on the device.

Before you begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. **configure terminal**
2. **no fips mode enable**
3. **exit**
4. (Optional) **show fips status**

5. **copy running-config startup-config**
6. **reload**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no fips mode enable** **Example:** `switch(config)# no fips mode enable`	Disables FIPS mode.

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

Step 4	(Optional) **show fips status**
	Example:
	`switch# show fips status`
	`FIPS mode is disabled`
		Displays the status of FIPS mode.

Step 5	Required: **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.
Step 6	Required: **reload** **Example:** `switch# reload`	Reloads the Cisco NX-OS device.

Related Topics

Enabling FIPS Mode, on page 20

Verifying the FIPS Configuration

To display FIPS configuration information, perform one of the following tasks:

Command	Purpose
show fips status	Displays the status of the FIPS feature.

For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuration Example for FIPS

The following example shows how to enable FIPS mode:

```
config terminal
fips mode enable
show fips status
exit
copy running-config startup-config
reload
```

Additional References for FIPS

This section includes additional information related to implementing FIPS.

Related Documents

Related Topic	Document Title
Cisco NX-OS licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
VDC configuration	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*

Standards

Standards	Title
FIPS 140-2	Security Requirements for Cryptographic Modules

Feature History for FIPS

This table lists the release history for this feature.

Table 3: Feature History for FIPS

Feature Name	Releases	Feature Information
FIPS	6.1(1)	Added support for digital image signing on switches that contain the Supervisor 2 module.
FIPS	6.1(1)	Updated FIPS guidelines for M2 Series modules.

Feature Name	Releases	Feature Information
FIPS	6.0(1)	Updated FIPS guidelines for F2 Series modules.
FIPS	5.1(1)	This feature was introduced.

CHAPTER 4

Configuring AAA

This chapter describes how to configure authentication, authorization, and accounting (AAA) on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About AAA

This section includes information about AAA on Cisco NX-OS devices.

AAA Security Services

The AAA feature allows you to verify the identity of, grant access to, and track the actions of users managing a Cisco NX-OS device. Cisco NX-OS devices support Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System Plus (TACACS+) protocols.

Based on the user ID and password combination that you provide, Cisco NX-OS devices 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 Cisco NX-OS device 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, depending on the security protocol that you select, encryption.

Authentication is the process of verifying the identity of the person or device accessing the Cisco NX-OS device, which is based on the user ID and password combination provided by the entity trying to access the Cisco NX-OS device. Cisco NX-OS devices allow you to perform local authentication (using the local lookup database) or remote authentication (using one or more RADIUS or TACACS+ servers).

Authorization

Provides access control.AAA authorization is the process of assembling a set of attributes that describe what the user is authorized to perform. Authorization in the Cisco NX-OS software 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.

Accounting

Provides the method for collecting information, logging the information locally, and sending the information to the AAA server for billing, auditing, and reporting.

The accounting feature tracks and maintains a log of every management session used to access the Cisco NX-OS device. You can use this information to generate reports for troubleshooting and auditing purposes. You can store accounting logs locally or send them to remote AAA servers.

Note The Cisco NX-OS software supports authentication, authorization, and accounting independently. For example, you can configure authentication and authorization without configuring accounting.

Related Topics

Configuring Command Authorization on TACACS+ Servers, on page 119

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:

- It is easier to manage user password lists for each Cisco NX-OS device in the fabric.
- AAA servers are already deployed widely across enterprises and can be easily used for AAA services.
- You can centrally manage the accounting log for all Cisco NX-OS devices in the fabric.
- It is easier to manage user attributes for each Cisco NX-OS device in the fabric than using the local databases on the Cisco NX-OS devices.

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. The purpose of a server group is to provide for failover servers in case 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, then that server group option is considered a failure. If required, you can specify multiple server groups. If the Cisco NX-OS device encounters errors from the servers in the first group, it tries the servers in the next server group.

AAA Service Configuration Options

The AAA configuration in Cisco NX-OS devices is service based, which means that you can have separate AAA configurations for the following services:

- User Telnet or Secure Shell (SSH) login authentication
- Console login authentication
- Cisco TrustSec authentication
- 802.1X authentication
- Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) authentication for Network Admission Control (NAC)
- User management session accounting
- 802.1X accounting

This table provides the related CLI command for each AAA service configuration option.

Table 4: AAA Service Configuration Commands

AAA Service Configuration Option	Related Command
Telnet or SSH login	**aaa authentication login default**
Fallback to local authentication for the default login.	**aaa authentication login default fallback error local**
Console login	**aaa authentication login console**

AAA Service Configuration Option	Related Command
Cisco TrustSec authentication	**aaa authentication cts default**
802.1X authentication	**aaa authentication dot1x default**
EAPoUDP authentication	**aaa authentication eou default**
User session accounting	**aaa accounting default**
802.1X accounting	**aaa accounting dot1x default**

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

All RADIUS servers

Uses the global pool of RADIUS servers for authentication.

Specified server groups

Uses specified RADIUS, TACACS+, or LDAP server groups you have configured for authentication.

Local

Uses the local username or password database for authentication.

None

Specifies that no AAA authentication be used.

Note If you specify the all RADIUS servers method, rather than a specified server group method, the Cisco NX-OS device chooses 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 NX-OS device.

This table shows the AAA authentication methods that you can configure for the AAA services.

Table 5: AAA Authentication Methods for AAA Services

AAA Service	AAA Methods
Console login authentication	Server groups, local, and none
User login authentication	Server groups, local, and none
Cisco TrustSec authentication	Server groups only
802.1X authentication	Server groups only
EAPoUDP authentication	Server groups only
User management session accounting	Server groups and local
802.1X accounting	Server groups and local

Note For console login authentication, user login authentication, and user management session accounting, the Cisco NX-OS device tries each option in the order specified. The local option is the default method when other configured options fail. You can disable the local option for the console or default login by using the **no aaa authentication login** {**console** | **default**} **fallback error local** command.

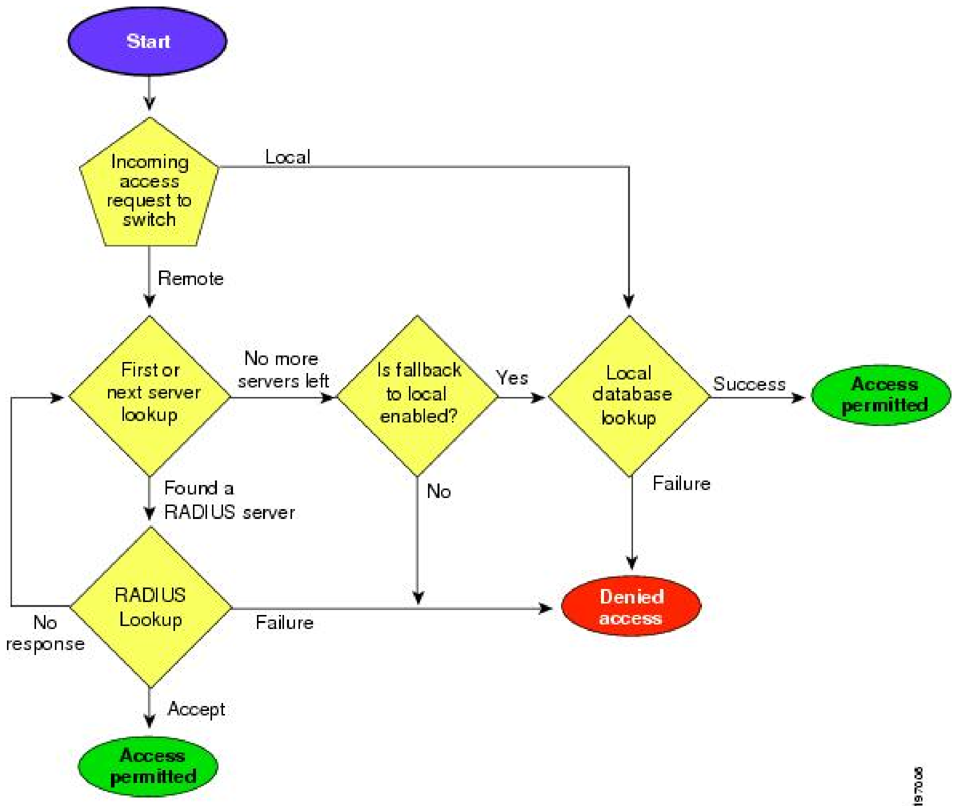
Related Topics

Configuring 802.1X, on page 263
Configuring NAC, on page 297

Authentication and Authorization Process for User Login

Figure 1: Authorization and Authentication Flow for User Login

This figure shows a flow chart of the authentication and authorization process for user login.



Note This diagram is applicable only to username password SSH authentication. It does not apply to public key SSH authentication. All username password SSH authentication goes through AAA.

The following list explains the process:

- When you log in to the required Cisco NX-OS device, you can use the Telnet, SSH, or console login options.

- When you have configured the AAA server groups using the server group authentication method, the Cisco NX-OS device sends an authentication request to the first AAA server in the group as follows:
    - If the AAA server fails to respond, 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, unless fallback to local is disabled for the console login.
- If the Cisco NX-OS device successfully authenticates you through a remote AAA server, then the following possibilities apply:
    - If the AAA server protocol is RADIUS, then user roles specified in the cisco-av-pair attribute are downloaded with an authentication response.
    - If the AAA server protocol is TACACS+, then another request is sent to the same server to get the user roles specified as custom attributes for the shell.
    - If the user roles are not successfully retrieved from the remote AAA server, then the user is assigned with the vdc-operator role.
- If your username and password are successfully authenticated locally, the Cisco NX-OS device logs you in and assigns you the roles configured in the local database.

Note "No more server groups left" means that there is no response from any server in all server groups. "No more servers left" means that there is no response from any server within this server group.

AES Password Encryption and Master Encryption Keys

You can enable strong, reversible 128-bit Advanced Encryption Standard (AES) password encryption, also known as type-6 encryption. To start using type-6 encryption, you must enable the AES password encryption feature and configure a master encryption key, which is used to encrypt and decrypt passwords.

After you enable AES password encryption and configure a master key, all existing and newly created clear-text passwords for supported applications (currently RADIUS and TACACS+) are stored in type-6 encrypted format, unless you disable type-6 password encryption. You can also configure Cisco NX-OS to convert all existing weakly encrypted passwords to type-6 encrypted passwords.

Related Topics

Configuring a Master Key and Enabling the AES Password Encryption Feature, on page 43
Configuring Global RADIUS Keys, on page 69
Configuring a Key for a Specific RADIUS Server, on page 71
Configuring Global TACACS+ Keys, on page 102
Configuring a Key for a Specific TACACS+ Server, on page 103

Virtualization Support for AAA

All AAA configuration and operations are local to the virtual device context (VDC), except the default console methods and the AAA accounting log. The configuration and operation of the AAA authentication methods for the console login apply only to the default VDC. The AAA accounting log is only in the default VDC. You can display the contents from any VDC, but you must clear it in the default VDC.

For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Prerequisites for AAA

Remote AAA servers have the following prerequisites:

- Ensure that at least one RADIUS, TACACS+, or LDAP server is reachable through IP.
- Ensure that the Cisco NX-OS device is configured as a client of the AAA servers.
- Ensure that the secret key is configured on the Cisco NX-OS device and the remote AAA servers.
- Ensure that the remote server responds to AAA requests from the Cisco NX-OS device.

Related Topics

Configuring RADIUS Server Hosts, on page 68
Configuring TACACS+ Server Hosts, on page 100
Configuring LDAP Server Hosts, on page 144
Manually Monitoring RADIUS Servers or Groups, on page 88
Manually Monitoring TACACS+ Servers or Groups, on page 130

Guidelines and Limitations for AAA

AAA has the following guidelines and limitations:

- If you have a user account configured on the local Cisco NX-OS device that has the same name as a remote user account on an AAA server, the Cisco NX-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.

Default Settings for AAA

This table lists the default settings for AAA parameters.

Table 6: Default AAA Parameter Settings

Parameters	Default
Console authentication method	local
Default authentication method	local

Parameters	Default
Login authentication failure messages	Disabled
CHAP authentication	Disabled
MSCHAP authentication	Disabled
Default accounting method	local
Accounting log display length	250 KB

Configuring AAA

This section describes the tasks for configuring AAA on Cisco NX-OS devices.

Note 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.

Process for Configuring AAA

Follow these steps to configure AAA authentication and accounting:

1. If you want to use remote RADIUS, TACACS+, or LDAP servers for authentication, configure the hosts on your Cisco NX-OS device.
2. Configure console login authentication methods.
3. Configure default login authentication methods for user logins.
4. Configure default AAA accounting default methods.

Related Topics

Configuring RADIUS, on page 61
Configuring TACACS+, on page 93
Configuring LDAP, on page 137
Configuring Console Login Authentication Methods, on page 32
Configuring Default Login Authentication Methods, on page 34
Configuring AAA Accounting Default Methods, on page 46
Configuring AAA Authentication Methods for 802.1X, on page 274
Enabling the Default AAA Authenication Method for EAPoUDP, on page 311

Configuring Console Login Authentication Methods

This section describes how to configure the authentication methods for the console login.

The authentication methods include the following:

- Global pool of RADIUS servers
- Named subset of RADIUS, TACACS+, or LDAP servers
- Local database on the Cisco NX-OS device
- Username only (none)

The default method is local, but you have the option to disable it.

Note The configuration and operation of AAA for the console login apply only to the default VDC.

Note The **group radius** and **group** *server-name* forms of the **aaa authentication** command refer to 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.

Note If you perform a password recovery when remote authentication is enabled, local authentication becomes enabled for console login as soon as the password recovery is done. As a result, you can log into the Cisco NX-OS device through the console port using the new password. After login, you can continue to use local authentication, or you can enable remote authentication after resetting the admin password configured at the AAA servers. For more information about the password recovery process, see the *Password Recovery Procedure for Cisco NX-OS*.

Before you begin

Ensure that you are in the default VDC.

Configure RADIUS, TACACS+, or LDAP server groups, as needed.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login console** {**group** *group-list* [**none**] | **local** | **none**}
3. **exit**
4. (Optional) **show aaa authentication**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

	Command or Action	Purpose
Step 2	**aaa authentication login console** {**group** *group-list* [**none**] | **local** | **none**} **Example:** `switch(config)# aaa authentication login console group radius`	Configures login authentication methods for the console. 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 RADIUS, TACACS+, or LDAP servers for authentication. The **local** method uses the local database for authentication, and the **none** method specifies that no AAA authentication be used. The default console login method is **local**, which is used when no methods are configured or when all the configured methods fail to respond, unless fallback to local is disabled for the console login.

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

Step 4	(Optional) **show aaa authentication** **Example:** `switch# show aaa authentication`	Displays the configuration of the console login authentication methods.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring RADIUS Server Groups, on page 72
Configuring TACACS+ Server Groups, on page 105
Configuring LDAP Server Groups, on page 146
Disabling Fallback to Local Authentication, on page 36

Configuring Default Login Authentication Methods

The authentication methods include the following:

- Global pool of RADIUS servers
- Named subset of RADIUS, TACACS+, or LDAP servers
- Local database on the Cisco NX-OS device

- Username only

The default method is local, but you have the option to disable it.

Before you begin

Configure RADIUS, TACACS+, or LDAP server groups, as needed.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login default** { **fallback error local** |**group** *group-list* [**none**] | **local** | **none**}
3. **exit**
4. (Optional) **show aaa authentication**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	**aaa authentication login default** { **fallback error local** |**group** *group-list* [**none**] | **local** | **none**} **Example:** `switch(config)# aaa authentication login default group radius`	Configures the default authentication methods. The **fallback error local** enables fallback to local authentication for the default login if remote authentication is configured and all AAA servers are unreachable. Fallback to local authentication is enabled by default. **Note** Disabling fallback to local authentication can lock your Cisco NX-OS device, forcing you to perform a password recovery in order to gain access. To prevent being locked out of the device, we recommend disabling fallback to local authentication for only the default login or the console login, not both. 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 RADIUS, TACACS+, or LDAP servers for authentication. The **local** method uses the local database for authentication, and the **none** method specifies that no AAA authentication be used. The default login method is **local**, which is used when no methods are configured or when all the configured

	Command or Action	Purpose
		methods fail to respond, unless fallback to local is disabled for the console login. You can configure one of the following: • AAA authentication groups • AAA authentication groups with no authentication • Local authentication • No authentication **Note** The **local** keyword is not supported (and is not required) when configuring AAA authentication groups because local authentication is the default if remote servers are unreachable. For example, if you configure **aaa authentication login default group g1**, local authentication is tried if you are unable to authenticate using AAA group g1. In contrast, if you configure **aaa authentication login default group g1 none**, no authentication is performed if you are unable to authenticate using AAA group g1.

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

Step 4	(Optional) **show aaa authentication** **Example:** `switch# show aaa authentication`	Displays the configuration of the default login authentication methods.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring RADIUS Server Groups, on page 72
Configuring TACACS+ Server Groups, on page 105
Configuring LDAP Server Groups, on page 146
Disabling Fallback to Local Authentication, on page 36

Disabling Fallback to Local Authentication

By default, if remote authentication is configured for console or default login and all AAA servers are unreachable (resulting in an authentication error), the Cisco NX-OS device falls back to local authentication to ensure that users are not locked out of the device. However, you can disable fallback to local authentication in order to increase security.

Caution Disabling fallback to local authentication can lock your Cisco NX-OS device, forcing you to perform a password recovery in order to gain access. To prevent being locked out of the device, we recommend that you disable fallback to local authentication for only the default login or the console login, not both.

Note The configuration and operation of the AAA for the console login apply only to the default VDC.

Before you begin

Ensure that you are in the default VDC before configuring remote authentication for the console login. You can configure remote authentication for the default login on a per-VDC basis.

Configure remote authentication for the console or default login.

SUMMARY STEPS

1. **configure terminal**
2. **no aaa authentication login** {**console** | **default**} **fallback error local**
3. (Optional) **exit**
4. (Optional) **show aaa authentication**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	**no aaa authentication login** {**console** | **default**} **fallback error local** **Example:** `switch(config)# no aaa authentication login console fallback error local`	Disables fallback to local authentication for the console or default login if remote authentication is configured and all AAA servers are unreachable. The following message appears when you disable fallback to local authentication: `“WARNING!!! Disabling fallback can lock your switch.”`

Step 3	(Optional) **exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

	Command or Action	Purpose
Step 4	(Optional) **show aaa authentication** **Example:** `switch# show aaa authentication`	Displays the configuration of the console and default login authentication methods.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring Console Login Authentication Methods, on page 32
Configuring Default Login Authentication Methods, on page 34

Enabling the Default User Role for AAA Authentication

You can allow remote users who do not have a user role to log in to the Cisco NX-OS device through a RADIUS or TACACS+ remote authentication server using a default user role. When you disable the AAA default user role feature, remote users who do not have a user role cannot log in to the device.

You can enable or disable this feature for the VDC as needed. For the default VDC, the default role is network-operator. For nondefault VDCs, the default VDC is vdc-operator.

Before you begin

Make sure that you are in the correct VDC. To switch VDCs, use the **switchto vdc** command.

SUMMARY STEPS

1. **configure terminal**
2. **aaa user default-role**
3. **exit**
4. (Optional) **show aaa user default-role**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	**aaa user default-role** **Example:** `switch(config)# aaa user default-role`	Enables the default user role for AAA authentication. The default is enabled. You can disable the default user role feature by using the **no** form of this command.

	Command or Action	Purpose

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

Step 4	(Optional) **show aaa user default-role** **Example:** `switch# show aaa user default-role`	Displays the AAA default user role configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring User Accounts and RBAC, on page 235

Enabling Login Authentication Failure Messages

When you log in, the login is processed by rolling over to the local user database if the remote AAA servers do not respond. In such cases, the following messages display on the user's terminal if you have enabled login failure messages:

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

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

Before you begin

Make sure that you are in the correct VDC. To switch VDCs, use the **switchto vdc** command.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login error-enable**
3. **exit**
4. (Optional) **show aaa authentication**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

	Command or Action	Purpose
Step 2	**aaa authentication login error-enable** **Example:** `switch(config)# aaa authentication login error-enable`	Enables login authentication failure messages. The default is disabled.

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

Step 4	(Optional) **show aaa authentication** **Example:** `switch# show aaa authentication`	Displays the login failure message configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling CHAP Authentication

The Cisco NX-OS software supports the Challenge Handshake Authentication Protocol (CHAP), a challenge-response authentication protocol that uses the industry-standard Message Digest (MD5) hashing scheme to encrypt responses. You can use CHAP for user logins to a Cisco NX-OS device through a remote authentication server (RADIUS or TACACS+).

By default, the Cisco NX-OS device uses Password Authentication Protocol (PAP) authentication between the Cisco NX-OS device and the remote server. If you enable CHAP, you need to configure your RADIUS or TACACS+ server to recognize the CHAP vendor-specific attributes (VSAs).

This table shows the RADIUS and TACACS+ VSAs required for CHAP.

Table 7: CHAP RADIUS and TACACS+ VSAs

Vendor-ID Number	Vendor-Type Number	VSA	Description
311	11	CHAP-Challenge	Contains the challenge sent by an AAA server to a CHAP user. It can be used in both Access-Request and Access-Challenge packets.
211	11	CHAP-Response	Contains the response value provided by a CHAP user in response to the challenge. It is used only in Access-Request packets.

Before you begin

Disable AAA ASCII authentication for logins.

SUMMARY STEPS

1. **configure terminal**
2. **no aaa authentication login ascii-authentication**
3. **aaa authentication login chap enable**
4. (Optional) **exit**
5. (Optional) **show aaa authentication login chap**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	**no aaa authentication login ascii-authentication** **Example:** `switch(config)# no aaa authentication login ascii-authentication`	Disables ASCII authentication.
Step 3	**aaa authentication login chap enable** **Example:** `switch(config)# aaa authentication login chap enable`	Enables CHAP authentication. The default is disabled. **Note** You cannot enable both CHAP and MSCHAP or MSCHAP V2 on your Cisco NX-OS device.

Step 4	(Optional) **exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show aaa authentication login chap** **Example:** `switch# show aaa authentication login chap`	Displays the CHAP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Using AAA Server VSAs with Cisco NX-OS Devices, on page 47

Enabling MSCHAP or MSCHAP V2 Authentication

Microsoft Challenge Handshake Authentication Protocol (MSCHAP) is the Microsoft version of CHAP. The Cisco NX-OS software also supports MSCHAP Version 2 (MSCHAP V2). You can use MSCHAP for user logins to a Cisco NX-OS device through a remote authentication server (RADIUS or TACACS+). MSCHAP V2 only supports user logins to a Cisco NX-OS device through remote authentication RADIUS servers. If you configure a TACACS+ group with MSCHAP V2, the AAA default login authentication uses the next configured method, or the local method, if no other server group is configured.

Note The Cisco NX-OS software may display the following message:

" Warning: MSCHAP V2 is supported only with Radius."

This warning message is informational only and does not affect MSCHAP V2 operation with RADIUS.

By default, the Cisco NX-OS device uses Password Authentication Protocol (PAP) authentication between the Cisco NX-OS device and the remote server. If you enable MSCHAP or MSCHAP V2, you need to configure your RADIUS server to recognize the MSCHAP and MSCHAP V2 vendor-specific attributes (VSAs).

This table shows the RADIUS VSAs required for MSCHAP.

Table 8: MSCHAP and MSCHAP V2 RADIUS VSAs

Vendor-ID Number	Vendor-Type Number	VSA	Description
311	11	MSCHAP-Challenge	Contains the challenge sent by an AAA server to an MSCHAP or MSCHAP V2 user. It can be used in both Access-Request and Access-Challenge packets.
211	11	MSCHAP-Response	Contains the response value provided by an MSCHAP or MSCHAP V2 user in response to the challenge. It is only used in Access-Request packets.

Before you begin

Disable AAA ASCII authentication for logins.

SUMMARY STEPS

1. **configure terminal**
2. **no aaa authentication login ascii-authentication**
3. **aaa authentication login** {**mschap** | **mschapv2**} **enable**
4. **exit**
5. (Optional) **show aaa authentication login** {**mschap** | **mschapv2**}
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

	Command or Action	Purpose
Step 2	**no aaa authentication login ascii-authentication** **Example:** `switch(config)# no aaa authentication login ascii-authentication`	Disables ASCII authentication.
Step 3	**aaa authentication login** {**mschap** | **mschapv2**} **enable** **Example:** `switch(config)# aaa authentication login mschap enable`	Enables MSCHAP or MSCHAP V2 authentication. The default is disabled. **Note** You cannot enable both MSCHAP and MSCHAP V2 on your Cisco NX-OS device.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show aaa authentication login** {**mschap** | **mschapv2**} **Example:** `switch# show aaa authentication login mschap`	Displays the MSCHAP or MSCHAP V2 configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Using AAA Server VSAs with Cisco NX-OS Devices, on page 47

Configuring a Master Key and Enabling the AES Password Encryption Feature

You can configure a master key for type-6 encryption and enable the Advanced Encryption Standard (AES) password encryption feature.

SUMMARY STEPS

1. [**no**] **key config-key ascii**
2. **configure terminal**
3. [**no**] **feature password encryption aes**
4. (Optional) **show encryption service stat**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	[**no**] **key config-key ascii** **Example:**	Configures a master key to be used with the AES password encryption feature. The master key can contain between 16

	Command or Action	Purpose

	`switch# key config-key ascii`
	`New Master Key:`
	`Retype Master Key:`
		and 32 alphanumeric characters. You can use the **no** form of this command to delete the master key at any time.
		
		If you enable the AES password encryption feature before configuring a master key, a message appears stating that password encryption will not take place unless a master key is configured. If a master key is already configured, you are prompted to enter the current master key before entering a new master key.

Step 2	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 3	[**no**] **feature password encryption aes** **Example:** `switch(config)# feature password encryption aes`	Enables or disables the AES password encryption feature.
Step 4	(Optional) **show encryption service stat** **Example:** `switch(config)# show encryption service stat`	Displays the configuration status of the AES password encryption feature and the master key.
Step 5	Required: **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration. **Note** This command is necessary to synchronize the master key in the running configuration and the startup configuration.

Related Topics

Configuring Text for a Key, on page 596
Configuring Accept and Send Lifetimes for a Key, on page 598
AES Password Encryption and Master Encryption Keys, on page 30

Converting Existing Passwords to Type-6 Encrypted Passwords

You can convert existing plain or weakly encrypted passwords to type-6 encrypted passwords.

Before you begin

Ensure that you have enabled the AES password encryption feature and configured a master key.

SUMMARY STEPS

1. **encryption re-encrypt obfuscated**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**encryption re-encrypt obfuscated** **Example:** `switch# encryption re-encrypt obfuscated`	Converts existing plain or weakly encrypted passwords to type-6 encrypted passwords.

Converting Type-6 Encrypted Passwords Back to Their Original States

You can convert type-6 encrypted passwords back to their original states.

Before you begin

Ensure that you have configured a master key.

SUMMARY STEPS

1. **encryption decrypt type6**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**encryption decrypt type6**
	Example:
	`switch# encryption decrypt type6`
	`Please enter current Master Key:`
		Converts type-6 encrypted passwords back to their original states.

Deleting Type-6 Encrypted Passwords

You can delete all type-6 encrypted passwords from the Cisco NX-OS device.

SUMMARY STEPS

1. **encryption delete type6**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**encryption delete type6** **Example:** `switch# encryption delete type6`	Deletes all type-6 encrypted passwords.

Configuring AAA Accounting Default Methods

Cisco NX-OS software supports TACACS+ and RADIUS methods for accounting. Cisco NX-OS devices 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 NX-OS 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

Configure RADIUS or TACACS+ server groups, as needed.

SUMMARY STEPS

1. **configure terminal**
2. **aaa accounting default** {**group** *group-list* | **local**}
3. **exit**
4. (Optional) **show aaa accounting**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	**aaa accounting default** {**group** *group-list*	**local**} **Example:** `switch(config)# aaa accounting default group radius`	Configures the default accounting method. 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.

	Command or Action	Purpose
		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 groups fail to respond.

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

Step 4	(Optional) **show aaa accounting** **Example:** `switch# show aaa accounting`	Displays the configuration AAA accounting default methods.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring RADIUS Server Groups, on page 72
Configuring TACACS+ Server Groups, on page 105

Using AAA Server VSAs with Cisco NX-OS Devices

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

About VSAs

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:

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

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

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

VSA Format

The following VSA protocol options are supported by the Cisco NX-OS software:

Shell
: Protocol used in access-accept packets to provide user profile information.

Accounting
: Protocol 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 NX-OS software:

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. For example, if you belong to roles network-operator and vdc-admin, the value field would be network-operator vdc-admin. This subattribute is sent in the VSA portion of the Access-Accept frames from the RADIUS server, and it can only be used with the shell protocol value. These examples use the roles attribute:

```
shell:roles=network-operator vdc-admin
```

```
shell:roles*network-operator vdc-admin
```

The following examples show the roles attribute as supported by FreeRADIUS:

```
Cisco-AVPair = shell:roles=\network-operator vdc-admin\
```

```
Cisco-AVPair = shell:roles*\network-operator vdc-admin\
```

Note When you specify a VSA as shell:roles*"network-operator vdc-admin" or "shell:roles*\"network-operator vdc-admin\"", this VSA is flagged as an optional attribute and other Cisco devices ignore this attribute.

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, and it can only be used with the accounting protocol-related PDUs.

Specifying Cisco NX-OS 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 NX-OS 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.

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.

Related Topics

Configuring User Accounts and RBAC, on page 235

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.

SUMMARY STEPS

1. **configure terminal**
2. **[no] login block-for** *seconds* **attempts** *tries* **within** *seconds*
3. **[no] login quiet-mode access-class** {*acl-name* | *acl-number*}
4. **exit**
5. **show login failures**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**[no] login block-for** *seconds* **attempts** *tries* **within** *seconds* **Example:** `Switch(config)# login block-for 100 attempts 2 within 100`	Configures your Cisco NX-OS device for login parameters that help provide DoS detection. **Note** This command must be issued before any other login command can be used.
Step 3	**[no] login quiet-mode access-class** {*acl-name* | *acl-number*} **Example:** `Switch(config)# login quiet-mode access-class myacl`	(Optional) Although this command is optional, it is recommended that it be configured to specify an ACL that is to be applied to the device when the device switches to quiet mode. When the device is in quiet mode, all login requests are denied and the only available connection is through the console.
Step 4	**exit** **Example:** `Switch(config)# exit`	Exits to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show login failures** **Example:** `Switch# show login`	Displays login parameters. • **failures** --Displays information related only to failed login attempts.

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
TimeStamp
--------------------------------------------------------------------------------
admin                                    pts/0   bgl-ads-728.cisco.com   login
        Wed Jun 10 04:56:16 2015
admin                                    pts/0   bgl-ads-728.cisco.com   login
        Wed Jun 10 04:56:19 2015
--------------------------------------------------------------------------------
```

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.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication rejected** *attempts* **in** *seconds* **ban** *seconds*
3. **exit**
4. **show running config**
5. **show aaa local user blocked**
6. **clear aaa local user blocked** {**username** *user* | **all**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal`	Enters global configuration mode.
Step 2	**aaa authentication rejected** *attempts* **in** *seconds* **ban** *seconds* **Example:** `switch(config)# aaa authentication rejected 3 in 20 ban 300`	Configures login parameters to block an user. **Note** Use the **no aaa authentication rejected** command to revert to the default login parameters.
Step 3	**exit** **Example:** `switch(config)# exit`	Exits to privileged EXEC mode.
Step 4	**show running config** **Example:** `switch# show running config`	(Optional) Displays the login parameters.
Step 5	**show aaa local user blocked** **Example:** `switch# show aaa local user blocked`	(Optional) Displays the blocked local users.

	Command or Action	Purpose
Step 6	**clear aaa local user blocked** {**username** *user* | **all**} **Example:** `switch# clear aaa local user blocked username testuser`	(Optional) Clears the blocked local users. • **all**–Clears all the blocked local users.

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 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
```

Restricting Sessions Per User—Per User Per Login

Use this task to restrict the maximum sessions per user.

SUMMARY STEPS

1. **configure terminal**
2. **[no] user max-logins** *max-logins*
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**[no] user max-logins** *max-logins* **Example:** `Switch(config)# user max-logins 1`	Restricts the maximum sessions per user. The range is from 1 to 7. If you set the maximum login limit as 1, then only one session (telnet/SSH) is allowed per user.
Step 3	**exit** **Example:** `Switch(config)# exit`	Exits to privileged EXEC mode.

Configuring Passphrase and Locking User Accounts

Perform this task to configure passphrase lengths, time values, and locking user accounts.

SUMMARY STEPS

1. **userpassphrase** { **min-length** | **max-length** }
2. **userpassphrase** { **min-length** & **max-length** }
3. **show userpassphrase** {**min-length** | **max-length** | **length** }
4. **no userpassphrase** {**min-length** | **max-length** | **length** }
5. **show userpassphrase all**
6. **userpassphrase** { **default-lifetime** | **default-warntime** | **default-gracetime** }
7. **username** <*username*> **passphrase** { **lifetime** | **warntime** | **gracetime** }
8. **no username** <*username*> **passphrase** { **lifetime** | **warntime** | **gracetime** | **timevalues** }
9. **show username** <*username*> **passphrase timevalues**
10. **username** <*username*> **lock-user-account**
11. **username** <*username*> **expire-userpassphrase**
12. **show locked-users**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**userpassphrase** { **min-length** | **max-length** } **Example:** `Switch(config)# userpassphrase {  min-length <8 ? 127> | max-length <80 ? 127> }`	Admin is allowed to configure either minimum or maximum passphrase length
Step 2	**userpassphrase** { **min-length** & **max-length** } **Example:**	Admin is allowed to configure both minimum and maximum passphrase length

	Command or Action	Purpose
	`Switch(config)# userpassphrase {  min-length <8 ? 127> & max-length <80 ? 127> }`	
Step 3	**show userpassphrase** {**min-length** | **max-length** | **length** } **Example:** `Switch(config)# show userpassphrase {min-length | max-length | length }`	Using min-length or max-length option, user is allowed to view either minimum or maximum passphrase length configuration .Using length option, they can view complete passphrase length configuration.
Step 4	**no userpassphrase** {**min-length** | **max-length** | **length** } **Example:** `Switch(config)# userpassphrase {min-length | max-length | length }`	To reset the passphrase length configuration to default configuration
Step 5	**show userpassphrase all** **Example:** `Switch(config)# show userpassphrase all`	To list all the parameter values under userpassphrase
Step 6	**userpassphrase** { **default-lifetime** | **default-warntime** | **default-gracetime** } **Example:** `Switch(config)# userpassphrase {  default-lifetime | default-warntime | default-gracetime }`	Admin is allowed to update the default configurations
Step 7	**username** <*username*> **passphrase** { **lifetime** | **warntime** | **gracetime** } **Example:** `Switch(config)# username  <user1> passphrase { lifetime | warntime | gracetime }`	Admin can configure passphrase lifetimes for any user
Step 8	**no username** <*username*> **passphrase** { **lifetime** | **warntime** | **gracetime** | **timevalues** } **Example:** `Switch(config)# username <user1> passphrase { lifetime | warntime | gracetime | timevalues }`	Admin can reset passphrase lifetimes to default values for any user
Step 9	**show username** <*username*> **passphrase timevalues** **Example:** `Switch(config)# show username <user1> passphrase timevalues`	Any user can view his/her passphrase lifetimes configured and admin can view for any user
Step 10	**username** <*username*> **lock-user-account** **Example:** `Switch(config)# username <user1> lock-user-account`	Admin can lock any user account
Step 11	**username** <*username*> **expire-userpassphrase** **Example:**	Admin can set any userpassphrase to expire immediately

	Command or Action	Purpose
	`Switch(config)# username <user1> expire-userpassphrase`	
Step 12	**show locked-users** **Example:** `Switch(config)# show locked-users`	Admin can view and unlock all the locked users

Enabling the Password Prompt for User Name

SUMMARY STEPS

1. **configure terminal**
2. **[no] password prompt username**
3. **exit**

DETAILED STEPS

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

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

abd9d40020538acc363df3d1bae7d1df16841e4903fca2c07c7898bf4f549ef5
```

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.

SUMMARY STEPS

1. **configure terminal**
2. **generate type7_encrypted_secret**
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**generate type7_encrypted_secret** **Example:** `Switch(config)# generate type7_encrypted_secret`	Configures RADIUS and TACACS shared secret with key type 7. While generating an encrypted shared secret, user input is hidden. **Note** You can generate encrypted equivalent of plain text separately and can configure the encrypted shared secret later.
Step 3	**exit** **Example:** `Switch(config)# exit`	Exits to privileged EXEC mode.

Monitoring and Clearing the Local AAA Accounting Log

The Cisco NX-OS device maintains a local log for the AAA accounting activity. You can monitor this log and clear it.

Note The AAA accounting log is local to the default VDC. You can monitor the contents from any VDC, but you must clear it in the default VDC.

SUMMARY STEPS

1. **show accounting log** [*size* | **last-index** | **start-seqnum** *number* | **start-time** *year month day hh***:***mm***:***ss*]
2. (Optional) **clear accounting log** [**logflash**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show accounting log** [*size* | **last-index** | **start-seqnum** *number* | **start-time** *year month day hh***:***mm***:***ss*]	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 or Action	Purpose
	Example: `switch# show accounting log`	command output. The range is from 0 to 250000 bytes. You can also specify a starting sequence number or a starting time for the log output.The range of the starting index is from 1 to 1000000. Use the **last-index** keyword to display the value of the last index number in the accounting log file.
Step 2	(Optional) **clear accounting log** [**logflash**] **Example:** `switch# clear aaa accounting log`	Clears the accounting log contents. The **logflash** keyword clears the accounting log stored in the logflash for the current VDC.

Verifying the AAA Configuration

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

Command	Purpose
show aaa accounting	Displays AAA accounting configuration.
show aaa authentication [**login** {**ascii-authentication** | **chap** | **error-enable** | **mschap** | **mschapv2**}]	Displays AAA authentication login configuration information.
show aaa groups	Displays the AAA server group configuration.
show running-config aaa [**all**]	Displays the AAA configuration in the running configuration.
show startup-config aaa	Displays the AAA configuration in the startup configuration.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuration Examples for AAA

The following example shows how to configure AAA:

```
aaa authentication login default group radius
aaa authentication login console group radius
aaa accounting default group radius
```

Additional References for AAA

This section includes additional information related to implementing AAA.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
SNMP	*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

- CISCO-AAA-SERVER-MIB
- CISCO-AAA-SERVER-EXT-MIB

Feature History for AAA

This table lists the release history for this feature.

Table 9: Feature History for AAA

Feature Name	Releases	Feature Information
Login Block Per User	7.3(0)D1(1)	Added support for login block per user. Refer to the "Secure Login Enhancements" section.
Secure Login Enhancements	7.2(0)D1(1)	Added enhancements for secure login. Refer to the "Secure Login Enhancements" section.
AAA	6.0(1)	No change from Release 5.2.
AAA	5.2(1)	Added support for the Cisco Nexus 3000 Series Switches.
AAA	5.2(1)	No change from Release 5.1.

Feature Name	Releases	Feature Information
AAA	5.1(1)	No change from Release 5.0.
AAA authentication	5.0(2)	Added support for enabling or disabling AAA authentication for user logins.
AAA authentication	5.0(2)	Added support for remote users who do not have a user role to log in to the Cisco NX-OS device through a RADIUS or TACACS+ remote authentication server using a default user role.
Login authentication	5.0(2)	Added support for enabling or disabling login authentication failure messages.
CHAP authentication	5.0(2)	Added support for enabling or disabling CHAP authentication.
Local authentication	5.0(2)	Added support for enabling fallback to local authentication when remote authentication fails.
Local authentication	5.0(2)	Added support for disabling fallback to local authentication.
MSCHAP V2 authentication	4.2(1)	Added support for enabling or disabling MSCHAP V2 authentication.
AAA	4.2(1)	No change from Release 4.1.

CHAPTER 5

Configuring RADIUS

This chapter describes how to configure the Remote Access Dial-In User Service (RADIUS) protocol on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About RADIUS

The RADIUS distributed client/server system allows you to secure networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco NX-OS 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 NX-OS device with RADIUS to the network. This action might be the first step when you make a transition to a 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 NX-OS device to better manage ports using their existing RADIUS solutions and to efficiently manage shared resources to offer different service-level agreements.

RADIUS Operation

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

- The user is prompted for and enters a username and password.
- The username and encrypted password are sent over the network to the RADIUS server.
- 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:

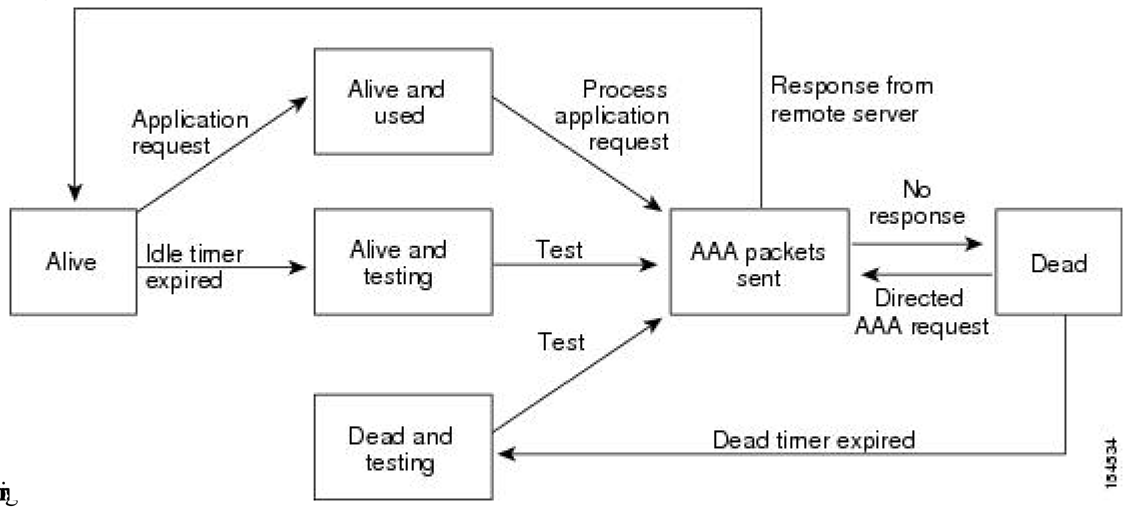
- Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IPv4 or IPv6 address, access list, and user timeouts.

RADIUS Server Monitoring

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

Figure 2: RADIUS Server States

This figure shows the states for RADIUS server



monitoring

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

RADIUS Configuration Distribution

Cisco Fabric Services (CFS) allows the Cisco NX-OS device to distribute the RADIUS configuration to other Cisco NX-OS devices in the network. When you enable CFS distribution for a feature on your device, the device belongs to a CFS region containing other devices in the network that you have also enabled for CFS distribution for the feature. CFS distribution for RADIUS is disabled by default.

Note You must explicitly enable CFS for RADIUS on each device to which you want to distribute configuration changes.

After you enable CFS distribution for RADIUS on your Cisco NX-OS device, the first RADIUS configuration command that you enter causes the Cisco NX-OS software to take the following actions:

- Creates a CFS session on your Cisco NX-OS device.

- Locks the RADIUS configuration on all Cisco NX-OS devices in the CFS region with CFS enabled for RADIUS.
- Saves the RADIUS configuration changes in a temporary buffer on the Cisco NX-OS device.

The changes stay in the temporary buffer on the Cisco NX-OS device until you explicitly commit them to be distributed to the devices in the CFS region. When you commit the changes, the Cisco NX-OS software takes the following actions:

- Applies the changes to the running configuration on your Cisco NX-OS device.
- Distributes the updated RADIUS configuration to the other Cisco NX-OS devices in the CFS region.
- Unlocks the RADIUS configuration in the devices in the CFS region.
- Terminates the CFS session.

CFS does not distribute the RADIUS server group configuration or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.

For detailed information on CFS, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.

Vendor-Specific Attributes

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:

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

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

When you use RADIUS servers for authentication on a Cisco NX-OS 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 NX-OS software:

Shell
: Protocol used in access-accept packets to provide user profile information.

Accounting
: Protocol used in accounting-request packets. If a value contains any white spaces, you should enclose the value within double quotation marks.

The Cisco NX-OS software 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 space. For example, if the user belongs to roles network-operator and vdc-admin, the value field would be network-operator vdc-admin. This subattribute, which the RADIUS server sends in the

VSA portion of the Access-Accept frames, can only be used with the shell protocol value. The following examples show the roles attribute that is supported by the Cisco Access Control Server (ACS):

```
shell:roles=network-operator vdc-admin

shell:roles*"network-operator vdc-admin
```

The following examples show the roles attribute that is supported by FreeRADIUS:

```
Cisco-AVPair = shell:roles=\network-operator vdc-admin\

Cisco-AVPair = shell:roles*\network-operator vdc-admin\
```

Note When you specify a VSA as shell:roles*"network-operator vdc-admin" or "shell:roles*\"network-operator vdc-admin\"", this VSA is flagged as an optional attribute and other Cisco devices ignore this attribute.

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).

Virtualization Support for RADIUS

RADIUS configuration and operation are local to the virtual device context (VDC). For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

The Cisco NX-OS device uses virtual routing and forwarding instances (VRFs) to access the RADIUS servers. For more information on VRFs, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

Prerequisites for RADIUS

RADIUS has the following prerequisites:

- Obtain IPv4 or IPv6 addresses or hostnames for the RADIUS servers.
- Obtain keys from the RADIUS servers.
- Ensure that the Cisco NX-OS device is configured as a RADIUS client of the AAA servers.

Guidelines and Limitations for RADIUS

RADIUS has the following guidelines and limitations:

- You can configure a maximum of 64 RADIUS servers on the Cisco NX-OS device.

- If you have a user account configured on the local Cisco NX-OS device that has the same name as a remote user account on an AAA server, the Cisco NX-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.
- Only the RADIUS protocol supports one-time passwords.

Default Settings for RADIUS

This table lists the default settings for RADIUS parameters.

Table 10: Default RADIUS Parameter Settings

Parameters	Default
Server roles	Authentication and accounting
Dead timer interval	0 minutes
Retransmission count	1
Retransmission timer interval	5 seconds
Authentication port	1812
Accouinting port	1813
Idle timer interval	0 minutes
Periodic server monitoring username	test
Periodic server monitoring password	test

Configuring RADIUS Servers

This section describes how to configure RADIUS servers on a Cisco NX-OS device.

Note 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.

RADIUS Server Configuration Process

1. If needed, enable CFS configuration distribution for RADIUS.
2. Establish the RADIUS server connections to the Cisco NX-OS device.
3. Configure the RADIUS secret keys for the RADIUS servers.

4. If needed, configure RADIUS server groups with subsets of the RADIUS servers for AAA authentication methods.
5. If needed, configure any of the following optional parameters:
    - Dead-time interval
    - RADIUS server specification allowed at user login
    - Timeout interval
    - TCP port
6. (Optional) If RADIUS distribution is enabled, commit the RADIUS configuration to the fabric.

Related Topics

Configuring RADIUS Server Hosts, on page 68
Configuring Global RADIUS Keys, on page 69

Enabling RADIUS Configuration Distribution

Only Cisco NX-OS devices that have distribution enabled for RADIUS can participate in the distribution of the RADIUS configuration changes in the CFS region.

Before you begin

Ensure that CFS distribution is enabled.

SUMMARY STEPS

1. **configure terminal**
2. **radius distribute**
3. **exit**
4. (Optional) **show radius status**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**radius distribute** **Example:** `switch(config)# radius distribute`	Enable RADIUS configuration distribution. The default is disabled.
Step 3	**exit** **Example:**	Exits configuration mode.

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	
Step 4	(Optional) **show radius status** **Example:** `switch(config)# show radius status`	Displays the RADIUS CFS distribution configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring RADIUS Server Hosts

To access a remote RADIUS server, you must configure the IP address or hostname of a RADIUS server. You can configure up to 64 RADIUS servers.

Note By default, when you configure a RADIUS server IP address or hostname of the Cisco NX-OS device, the RADIUS server is added to the default RADIUS server group. You can also add the RADIUS server to another RADIUS server group.

Before you begin

Ensure that the server is already configured as a member of the server group.

Ensure that the server is configured to authenticate RADIUS traffic.

Ensure that the Cisco NX-OS device is configured as a RADIUS client of the AAA servers.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*}
3. (Optional) **show radius** {**pending** | **pending-diff**}
4. (Optional) **radius commit**
5. **exit**
6. (Optional) **show radius-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **Example:** `switch(config)# radius-server host 10.10.1.1`	Specifies the IPv4 or IPv6 address or hostname for a RADIUS server to use for authentication.
Step 3	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	Displays the RADIUS configuration pending for distribution.
Step 4	(Optional) **radius commit** **Example:** `switch(config)# radius commit`	Applies the RADIUS configuration changes in the temporary database to the running configuration and distributes the RADIUS configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 6	(Optional) **show radius-server** **Example:** `switch# show radius-server`	Displays the RADIUS server configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring a Key for a Specific RADIUS Server, on page 71

Configuring Global RADIUS Keys

You can configure RADIUS keys for all servers used by the Cisco NX-OS device. A RADIUS key is a shared secret text string between the Cisco NX-OS device and the RADIUS server hosts.

Note CFS does not distribute RADIUS keys.

Before you begin

Obtain the RADIUS key values for the remote RADIUS servers.

Configure the RADIUS key on the remote RADIUS servers.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server key** [**0** | **6** | **7**] *key-value*
3. **exit**
4. (Optional) **show radius-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**radius-server key** [**0** | **6** | **7**] *key-value* **Example:** `switch(config)# radius-server key 0 QsEfThUkO`	Specifies a RADIUS key for all RADIUS servers. You can specify that the *key-value* is in clear text format (**0**), is type-6 encrypted (**6**), or is type-7 encrypted (**7**). The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters. By default, no RADIUS key is configured.

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

Step 4	(Optional) **show radius-server** **Example:** `switch# show radius-server`	Displays the RADIUS server configuration. **Note** The RADIUS keys are saved in encrypted form in the running configuration. Use the **show running-config** command to display the encrypted RADIUS keys.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

AES Password Encryption and Master Encryption Keys, on page 30
Configuring RADIUS Server Groups, on page 72
RADIUS Configuration Distribution, on page 63

Configuring a Key for a Specific RADIUS Server

You can configure a key on the Cisco NX-OS device for a specific RADIUS server. A RADIUS key is a secret text string shared between the Cisco NX-OS device and a specific RADIUS server.

Before you begin

Configure one or more RADIUS server hosts.

Obtain the key value for the remote RADIUS server.

Configure the key on the RADIUS server.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **6** | **7**] *key-value*
3. **exit**
4. (Optional) **show radius-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **6** | **7**] *key-value* **Example:** `switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg`	Specifies a RADIUS key for a specific RADIUS server. You can specify that the *key-value* is in clear text format (**0**), is type-6 encrypted (**6**), or is type-7 encrypted (**7**). The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters. This RADIUS key is used instead of the global RADIUS key.

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

Step 4	(Optional) **show radius-server** **Example:** `switch# show radius-server`	Displays the RADIUS server configuration. **Note** The RADIUS keys are saved in encrypted form in the running configuration. Use the **show running-config** command to display the encrypted RADIUS keys.

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

Related Topics

AES Password Encryption and Master Encryption Keys, on page 30
Configuring RADIUS Server Hosts, on page 68

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. You can configure up to 100 server groups in a VDC.

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

Note CFS does not distribute RADIUS server group configurations.

Before you begin

Ensure that all servers in the group are RADIUS servers.

SUMMARY STEPS

1. **configure terminal**
2. **aaa group server radius** *group-name*
3. **server** {*ipv4-address* | *ipv6-address* | *host-name*}
4. (Optional) **deadtime** *minutes*
5. (Optional) **server** {*ipv4-address* | *ipv6-address* | *host-name*}
6. (Optional) **use-vrf** *vrf-name*
7. **exit**
8. (Optional) **show radius-server groups** [*group-name*]
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**aaa group server radius** *group-name*
	Example:
	`switch(config)# aaa group server radius RadServer`
	`switch(config-radius)#`
		Creates a RADIUS server group and enters the RADIUS server group configuration submode for that group. The *group-name* argument is a case-sensitive alphanumeric string with a maximum length of 127 characters.

Step 3	**server** {*ipv4-address* | *ipv6-address* | *host-name*} **Example:** `switch(config-radius)# server 10.10.1.1`	Configures the RADIUS server as a member of the RADIUS server group. If the specified RADIUS server is not found, configure it using the **radius-server host** command and retry this command.
Step 4	(Optional) **deadtime** *minutes* **Example:** `switch(config-radius)# deadtime 30`	Configures the monitoring dead time. The default is 0 minutes. The range is from 1 through 1440. **Note** 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.
Step 5	(Optional) **server** {*ipv4-address* | *ipv6-address* | *host-name*} **Example:** `switch(config-radius)# server 10.10.1.1`	Configures the RADIUS server as a member of the RADIUS server group. **Tip** If the specified RADIUS server is not found, configure it using the **radius-server host** command and retry this command.
Step 6	(Optional) **use-vrf** *vrf-name* **Example:** `switch(config-radius)# use-vrf vrf1`	Specifies the VRF to use to contact the servers in the server group.

Step 7	**exit**
	Example:
	`switch(config-radius)# exit`
	`switch(config)#`
		Exits configuration mode.

Step 8	(Optional) **show radius-server groups** [*group-name*] **Example:** `switch(config)# show radius-server groups`	Displays the RADIUS server group configuration.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring the RADIUS Dead-Time Interval, on page 84

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. By default, the Cisco NX-OS software uses any available interface.

SUMMARY STEPS

1. **configure terminal**
2. **ip radius source-interface** *interface*
3. **exit**
4. (Optional) **show radius-server**
5. (Optional) **copy running-config startup config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)`
		Enters global configuration mode.

Step 2	**ip radius source-interface** *interface* **Example:** `switch(config)# ip radius source-interface mgmt 0`	Configures the global source interface for all RADIUS server groups configured on the device.

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

Step 4	(Optional) **show radius-server** **Example:** `switch# show radius-server`	Displays the RADIUS server configuration information.
Step 5	(Optional) **copy running-config startup config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring RADIUS Server Groups, on page 72

Allowing Users to Specify a RADIUS Server at Login

By default, the Cisco NX-OS device forwards an authentication request based on the default AAA authentication method. You can configure the Cisco NX-OS device to allow the user to specify a VRF and RADIUS server to send the authentication request by enabling the directed-request option. If you enable this option, the user can log in as *username@vrfname***:***hostname*, where *vrfname* is the VRF to use and **hostname** is the name of a configured RADIUS server.

Note If you enable the directed-request option, the Cisco NX-OS device uses only the RADIUS method for authentication and not the default local method.

Note User-specified logins are supported only for Telnet sessions.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server directed-request**
3. (Optional) **show radius** {**pending** | **pending-diff**}
4. (Optional) **radius commit**
5. **exit**
6. (Optional) **show radius-server directed-request**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**radius-server directed-request** **Example:** `switch(config)# radius-server directed-request`	Allows users to specify a RADIUS server to send the authentication request when logging in. The default is disabled.
Step 3	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	Displays the RADIUS configuration pending for distribution.
Step 4	(Optional) **radius commit** **Example:** `switch(config)# radius commit`	Applies the RADIUS configuration changes in the temporary database to the running configuration and distributes the RADIUS configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

	Command or Action	Purpose
Step 6	(Optional) **show radius-server directed-request** **Example:** `switch# show radius-server directed-request`	Displays the directed request configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

RADIUS Configuration Distribution, on page 63

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 Cisco NX-OS device 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 NX-OS device waits for responses from RADIUS servers before declaring a timeout failure.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server retransmit** *count*
3. **radius-server timeout** *seconds*
4. (Optional) **show radius** {**pending** | **pending-diff**}
5. (Optional) **radius commit**
6. **exit**
7. (Optional) **show radius-server**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**radius-server retransmit** *count* **Example:** `switch(config)# radius-server retransmit 3`	Specifies the retransmission count for all RADIUS servers. The default retransmission count is 1 and the range is from 0 to 5.
Step 3	**radius-server timeout** *seconds* **Example:** `switch(config)# radius-server timeout 10`	Specifies the transmission timeout interval for RADIUS servers. The default timeout interval is 5 seconds and the range is from 1 to 60 seconds.

	Command or Action	Purpose
Step 4	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	Displays the RADIUS configuration pending for distribution.
Step 5	(Optional) **radius commit** **Example:** `switch(config)# radius commit`	Applies the RADIUS configuration changes in the temporary database to the running configuration and distributes the RADIUS configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 6	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 7	(Optional) **show radius-server** **Example:** `switch# show radius-server`	Displays the RADIUS server configuration.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

RADIUS Configuration Distribution, on page 63

Configuring the RADIUS Transmission Retry Count and Timeout Interval for a Server

By default, a Cisco NX-OS device retries a 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 Cisco NX-OS device waits for responses from RADIUS servers before declaring a timeout failure.

Before you begin

Configure one or more RADIUS server hosts.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **retransmit** *count*
3. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout** *seconds*
4. (Optional) **show radius** {**pending** | **pending-diff**}
5. (Optional) **radius commit**
6. **exit**

7. (Optional) **show radius-server**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **retransmit** *count* **Example:** `switch(config)# radius-server host server1 retransmit 3`	Specifies the retransmission count for a specific server. The default is the global value. **Note** The retransmission count value specified for a RADIUS server overrides the count specified for all RADIUS servers.
Step 3	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout** *seconds* **Example:** `switch(config)# radius-server host server1 timeout 10`	Specifies the transmission timeout interval for a specific server. The default is the global value. **Note** The timeout interval value specified for a RADIUS server overrides the interval value specified for all RADIUS servers.
Step 4	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	Displays the RADIUS configuration pending for distribution.
Step 5	(Optional) **radius commit** **Example:** `switch(config)# radius commit`	Applies the RADIUS configuration changes in the temporary database to the running configuration and distributes RADIUS configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 6	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 7	(Optional) **show radius-server** **Example:** `switch# show radius-server`	Displays the RADIUS server configuration.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring RADIUS Server Hosts, on page 68
RADIUS Configuration Distribution, on page 63

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 if there is a conflict with the default port.

Before you begin

Configure one or more RADIUS server hosts.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **acct-port** *udp-port*
3. (Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **accounting**
4. (Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **auth-port** *udp-port*
5. (Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **authentication**
6. (Optional) **show radius** {**pending** | **pending-diff**}
7. (Optional) **radius commit**
8. **exit**
9. (Optional) **show radius-server**
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **acct-port** *udp-port* **Example:** `switch(config)# radius-server host 10.10.1.1 acct-port 2004`	Specifies a UDP port to use for RADIUS accounting messages. The default UDP port is 1813. The range is from 0 to 65535.
Step 3	(Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **accounting** **Example:** `switch(config)# radius-server host 10.10.1.1 accounting`	Specifies to use the RADIUS server only for accounting purposes. The default is both accounting and authentication.

	Command or Action	Purpose
Step 4	(Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **auth-port** *udp-port* **Example:** `switch(config)# radius-server host 10.10.2.2 auth-port 2005`	Specifies a UDP port to use for RADIUS authentication messages. The default UDP port is 1812. The range is from 0 to 65535.
Step 5	(Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **authentication** **Example:** `switch(config)# radius-server host 10.10.2.2 authentication`	Specifies to use the RADIUS server only for authentication purposes. The default is both accounting and authentication.
Step 6	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	Displays the RADIUS configuration pending for distribution.
Step 7	(Optional) **radius commit** **Example:** `switch(config)# radius commit`	Applies the RADIUS configuration changes in the temporary database to the running configuration and distributes the RADIUS configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 8	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 9	(Optional) **show radius-server** **Example:** `switch(config)# show radius-server`	Displays the RADIUS server configuration.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring RADIUS Server Hosts, on page 68
RADIUS Configuration Distribution, on page 63

Configuring Global Periodic RADIUS Server Monitoring

You can monitor the availability of all RADIUS servers without having to configure the test parameters for each server individually. Any servers for which test parameters are not configured are monitored using the global level parameters.

Note Test parameters that are configured for individual servers take precedence over global test parameters.

The global configuration parameters include the username and password to use for the servers and an idle timer. The idle timer specifies the interval in which a RADIUS server receives no requests before the Cisco NX-OS 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 CFS does not distribute global RADIUS server group configurations.

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

Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Before you begin

Enable RADIUS.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}
3. **radius-server deadtime** *minutes*
4. **exit**
5. (Optional) **show radius-server**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**radius-server test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}	Specifies parameters for global server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes.

	Command or Action	Purpose
	Example: `switch(config)# radius-server test username user1 password Ur2Gd2BH idle-time 3`	**Note** For periodic RADIUS server monitoring, the idle timer value must be greater than 0.
Step 3	**radius-server deadtime** *minutes* **Example:** `switch(config)# radius-server deadtime 5`	Specifies the number of minutes before the Cisco NX-OS device checks a RADIUS server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 0 to 1440 minutes.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show radius-server** **Example:** `switch# show radius-server`	Displays the RADIUS server configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring Periodic RADIUS Server Monitoring on Individual Servers, on page 82

Configuring Periodic RADIUS Server Monitoring on Individual Servers

You can monitor the availability of individual RADIUS servers. The configuration 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 Cisco NX-OS 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 Test parameters that are configured for individual servers take precedence over global test parameters.

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.

Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, the Cisco NX-OS device does not perform periodic RADIUS server monitoring.

Before you begin

Enable RADIUS.

Add one or more RADIUS server hosts.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}
3. **radius-server deadtime** *minutes*
4. **exit**
5. (Optional) **show radius-server**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **Example:** `switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3`	Specifies parameters for individual server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes. **Note** For periodic RADIUS server monitoring, you must set the idle timer to a value greater than 0.
Step 3	**radius-server deadtime** *minutes* **Example:** `switch(config)# radius-server deadtime 5`	Specifies the number of minutes before the Cisco NX-OS device checks a RADIUS server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 1 to 1440 minutes.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show radius-server** **Example:** `switch# show radius-server`	Displays the RADIUS server configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring RADIUS Server Hosts, on page 68
Configuring Global Periodic RADIUS Server Monitoring, on page 80

Configuring the RADIUS Dead-Time Interval

You can configure the dead-time interval for all RADIUS servers. The dead-time interval specifies the time that the Cisco NX-OS 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.

Note 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.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server deadtime** *minutes*
3. (Optional) **show radius** {**pending** | **pending-diff**}
4. (Optional) **radius commit**
5. **exit**
6. (Optional) **show radius-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**radius-server deadtime** *minutes* **Example:** `switch(config)# radius-server deadtime 5`	Configures the dead-time interval. The default value is 0 minutes. The range is from 1 to 1440 minutes.
Step 3	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	Displays the RADIUS configuration pending for distribution.
Step 4	(Optional) **radius commit** **Example:** `switch(config)# radius commit`	Applies the RADIUS configuration changes in the temporary database to the running configuration and distributes the RADIUS configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

	Command or Action	Purpose

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 6	(Optional) **show radius-server** **Example:** `switch# show radius-server`	Displays the RADIUS server configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring RADIUS Server Groups, on page 72
RADIUS Configuration Distribution, on page 63

Configuring One-Time Passwords

One-time password (OTP) support is available for Cisco NX-OS devices through the use of RSA SecurID token servers. With this feature, users authenticate to a Cisco NX-OS device by entering both a personal identification number (or one-time password) and the token code being displayed at that moment on their RSA SecurID token.

Note The token code used for logging into the Cisco NX-OS device changes every 60 seconds. To prevent problems with device discovery, we recommend using different usernames that are present on the Cisco Secure ACS internal database.

Before you begin

On the Cisco NX-OS device, configure a RADIUS server host and remote default login authentication.

Ensure that the following are installed:

- Cisco Secure Access Control Server (ACS) version 4.2
- RSA Authentication Manager version 7.1 (the RSA SecurID token server)
- RSA ACE Agent/Client

No configuration (other than a RADIUS server host and remote authentication) is required on the Cisco NX-OS device to support one-time passwords. However, you must configure the Cisco Secure ACS as follows:

1. Enable RSA SecurID token server authentication.
2. Add the RSA SecurID token server to the Unknown User Policy database.

Committing the RADIUS Distribution

You can apply the RADIUS global and server-specific configuration stored in the temporary buffer to the running configuration across all devices in the fabric (including the originating device).

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **show radius** {**pending** | **pending-diff**}
3. **radius commit**
4. **exit**
5. (Optional) **show role session status**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	Displays the RADIUS configuration pending for distribution.
Step 3	**radius commit** **Example:** `switch(config)# radius commit`	Applies the RADIUS configuration changes in the temporary database to the running configuration and distributes the RADIUS configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show role session status** **Example:** `switch# show role session status`	Displays the user role CFS session status.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Applies the running configuration to the startup configuration.

Discarding the RADIUS Distribution Session

You can discard the temporary database of RADIUS changes and end the CFS distribution session.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **show radius** {**pending** | **pending-diff**}
3. **radius abort**
4. **exit**
5. (Optional) **show radius session status**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	Displays the RADIUS configuration pending for distribution.
Step 3	**radius abort** **Example:** `switch(config)# radius abort`	Discards the RADIUS configuration in the temporary storage and ends the session.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show radius session status** **Example:** `switch# show radius session status`	Displays the RADIUS CFS session status.

Clearing the RADIUS Distribution Session

You can clear the ongoing Cisco Fabric Services distribution session (if any) and unlock the fabric for the RADIUS feature.

SUMMARY STEPS

1. **clear radius session**
2. (Optional) **show radius session status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clear radius session** **Example:** `switch# clear radius session`	Clears the session and unlocks the fabric.
Step 2	(Optional) **show radius session status** **Example:** `switch# show radius session status`	Displays the RADIUS CFS session status.

Manually Monitoring RADIUS Servers or Groups

You can manually issue a test message to a RADIUS server or to a server group.

SUMMARY STEPS

1. **test aaa server radius** {*ipv4-address* | *ipv6-address* | *host-name*} [**vrf** *vrf-name*] *username password*
2. **test aaa group** *group-name username password*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**test aaa server radius** {*ipv4-address* | *ipv6-address* | *host-name*} [**vrf** *vrf-name*] *username password* **Example:** `switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH`	Sends a test message to a RADIUS server to confirm availability.
Step 2	**test aaa group** *group-name username password* **Example:** `switch# test aaa group RadGroup user2 As3He3CI`	Sends a test message to a RADIUS server group to confirm availability.

Verifying the RADIUS Configuration

To display RADIUS configuration information, perform one of the following tasks:

Command	Purpose
show radius {**status** | **pending** | **pending-diff**}	Displays the RADIUS Cisco Fabric Services distribution status and other details.
show running-config radius [**all**]	Displays the RADIUS configuration in the running configuration.

Command	Purpose
show startup-config radius	Displays the RADIUS configuration in the startup configuration.
show radius-server [*host-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	Displays all configured RADIUS server parameters.

For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Monitoring RADIUS Servers

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

Before you begin

Configure one or more RADIUS server hosts.

SUMMARY STEPS

1. **show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} **Example:** `switch# show radius-server statistics 10.10.1.1`	Displays the RADIUS statistics.

Related Topics

Configuring RADIUS Server Hosts, on page 68
Clearing RADIUS Server Statistics, on page 89

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.

SUMMARY STEPS

1. (Optional) **show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

2. **clear radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} **Example:** `switch# show radius-server statistics 10.10.1.1`	Displays the RADIUS server statistics on the Cisco NX-OS device.
Step 2	**clear radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} **Example:** `switch# clear radius-server statistics 10.10.1.1`	Clears the RADIUS server statistics.

Related Topics

Configuring RADIUS Server Hosts, on page 68

Configuration Example for RADIUS

The following example shows how to configure RADIUS:

```
radius-server key 7 "ToIkLhPpG"
radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
aaa group server radius RadServer
    server 10.10.1.1
```

Where to Go Next

You can now configure AAA authentication methods to include the server groups.

Additional References for RADIUS

This section describes additional information related to implementing RADIUS.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
VRF configuration	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
• CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for RADIUS

This table lists the release history for this feature.

Table 11: Feature History for RADIUS

Feature Name	Releases	Feature Information
RADIUS	6.0(1)	No change from Release 5.2.
RADIUS	5.2(1)	Added support for the Cisco Nexus 3000 Series Switches.
RADIUS	5.2(1)	Added type-6 encryption for RADIUS server keys.
RADIUS	5.1(1)	No change from Release 5.0.
RADIUS server groups	5.0(2)	Added support for configuring the global source interface for all RADIUS server groups.
RADIUS server groups	5.0(2)	Added support for configuring a source interface for a specific RADIUS server group.
Periodic server monitoring	5.0(2)	Added support for global periodic RADIUS server monitoring.
OTP	5.0(2)	Added support for one-time passwords.
RADIUS statistics	4.2(1)	Added support for clearing statistics for RADIUS server hosts.
RADIUS	4.2(1)	No change from Release 4.1.

CHAPTER 6

Configuring TACACS+

This chapter describes how to configure the Terminal Access Controller Access Control System Plus (TACACS+) protocol on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About TACACS+

The TACACS+ security protocol provides centralized validation of users attempting to gain access to a Cisco NX-OS device. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, 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 NX-OS 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 can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The TACACS+ client/server protocol uses TCP (TCP port 49) for transport requirements. Cisco NX-OS devices provide centralized authentication using the TACACS+ protocol.

TACACS+ Advantages

TACACS+ has the following advantages over RADIUS authentication:

- Provides independent AAA facilities. For example, the Cisco NX-OS 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.

TACACS+ Operation for User Login

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

Note 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 your mother's maiden name.

1. When the Cisco NX-OS device establishes a connection, it contacts the TACACS+ daemon to obtain the username and password.
2. The Cisco NX-OS device will eventually receive one of the following responses from the TACACS+ daemon:

   ACCEPT
   User authentication succeeds and service begins. If the Cisco NX-OS 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 NX-OS device. If the Cisco NX-OS device receives an ERROR response, the Cisco NX-OS device tries to use an alternative method for authenticating the user.

   After authentication, the user also undergoes an additional authorization phase if authorization has been enabled on the NX-OS device. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the Cisco NX-OS 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 or IPv6), access list, and user timeouts

Default TACACS+ Server Encryption Type and Secret Key

You must configure the TACACS+ secret key to authenticate the switch to the TACACS+ server. A secret key is a secret text string shared between the Cisco NX-OS 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 secret key for all TACACS+ server configurations on the Cisco NX-OS device to use.

You can override the global secret key assignment by explicitly using the **key** option when configuring an individual TACACS+ server.

Command Authorization Support for TACACS+ Servers

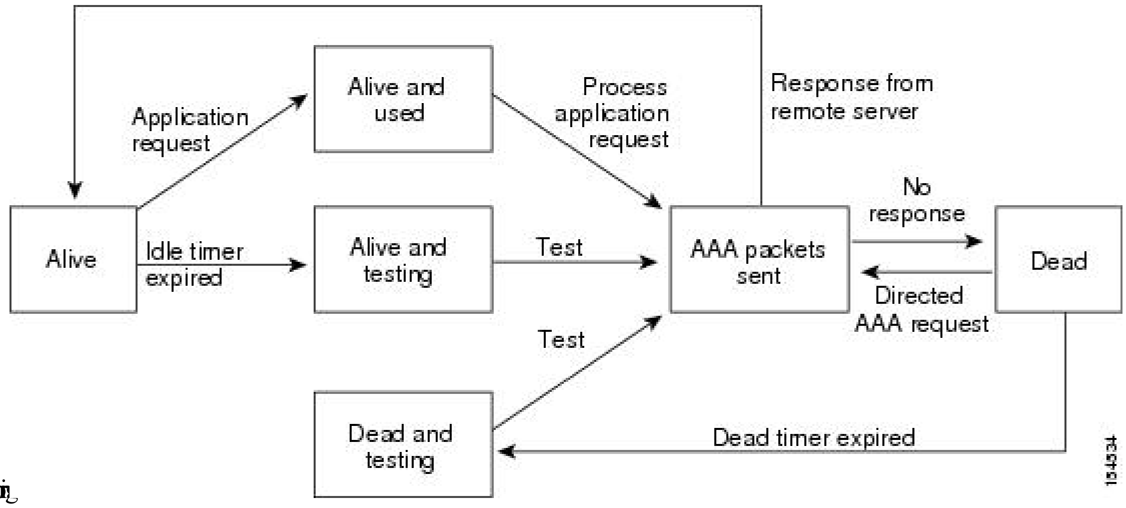
By default, command authorization is done against a local database in the Cisco NX-OS software when an authenticated user enters a command at the command-line interface (CLI). You can also verify authorized commands for authenticated users using TACACS+.

TACACS+ Server Monitoring

An unresponsive TACACS+ server can delay the processing of AAA requests. A Cisco NX-OS device can periodically monitor a TACACS+ server to check whether it is responding (or alive) to save time in processing AAA requests. The Cisco NX-OS device marks unresponsive TACACS+ servers as dead and does not send AAA requests to any dead TACACS+ servers. A Cisco NX-OS 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 its way. Whenever a TACACS+ server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Cisco NX-OS device displays an error message that a failure is taking place before it can impact performance.

Figure 3: TACACS+ Server States

This figure shows the server states for 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.

TACACS+ Configuration Distribution

Cisco Fabric Services (CFS) allows the Cisco NX-OS device to distribute the TACACS+ configuration and privilege roles to other Cisco NX-OS devices in the network. When you enable CFS distribution for a feature on your device, the device belongs to a CFS region containing other devices in the network that you have also enabled for CFS distribution for the feature. CFS distribution for TACACS+ is disabled by default.

> **Note** You must explicitly enable CFS for TACACS+ on each device to which you want to distribute configuration changes.

After you enable CFS distribution for TACACS+ on your Cisco NX-OS device, the first TACACS+ configuration command that you enter causes the Cisco NX-OS software to take the following actions:

- Creates a CFS session on your Cisco NX-OS device.
- Locks the TACACS+ configuration on all Cisco NX-OS devices in the CFS region with CFS enabled for TACACS+.
- Saves the TACACS+ configuration changes in a temporary buffer on the Cisco NX-OS device.

The changes stay in the temporary buffer on the Cisco NX-OS device until you explicitly commit them to be distributed to the devices in the CFS region. When you commit the changes, the Cisco NX-OS software takes the following actions:

- Applies the changes to the running configuration on your Cisco NX-OS device.

- Distributes the updated TACACS+ configuration to the other Cisco NX-OS devices in the CFS region.
- Unlocks the TACACS+ configuration in the devices in the CFS region.
- Terminates the CFS session.

CFS does not distribute the TACACS+ server group configuration, periodic TACACS+ server testing configurations, or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.

For detailed information on CFS, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.

Vendor-Specific Attributes for TACACS+

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific attributes (VSAs) between the network access server and the TACACS+ server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use.

Cisco VSA Format for TACACS+

The Cisco TACACS+ implementation supports one vendor-specific option using the format recommended in the IETF 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 = (equal sign) for mandatory attributes, and * (asterisk) indicates optional attributes.

When you use TACACS+ servers for authentication on a Cisco NX-OS device, the TACACS+ protocol directs the TACACS+ server to return user attributes, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

The following VSA protocol options are supported by the Cisco NX-OS software:

Shell
: Protocol used in access-accept packets to provide user profile information.

Accounting
: Protocol used in accounting-request packets. If a value contains any white spaces, you should enclose the value within double quotation marks.

The Cisco NX-OS software 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 space. For example, if the user belongs to roles network-operator and vdc-admin, the value field would be network-operator vdc-admin. This subattribute, which the TACACS+ server sends in the VSA portion of the Access-Accept frames, can only be used with the shell protocol value. The following examples show the roles attribute as supported by Cisco ACS:

```
shell:roles=network-operator vdc-admin

shell:roles*network-operator vdc-admin
```

Note When you specify a VSA as shell:roles*"network-operator vdc-admin", this VSA is flagged as an optional attribute and other Cisco devices ignore this attribute.

accountinginfo
Stores accounting information in addition to the attributes covered by a standard TACACS+ accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the TACACS+ client on the switch. It can be used only with the accounting protocol data units (PDUs).

Prerequisites for TACACS+

TACACS+ has the following prerequisites:

- Obtain the IPv4 or IPv6 addresses or hostnames for the TACACS+ servers.
- Obtain the secret keys from the TACACS+ servers, if any.
- Ensure that the Cisco NX-OS device is configured as a TACACS+ client of the AAA servers.

Guidelines and Limitations for TACACS+

TACACS+ has the following guidelines and limitations:

- You may get the following error message sporadically after you have configured a TACACS+ server host followed by the AAA configuration to actually use the host:

  ```
  %TACACS-3-TACACS_ERROR_MESSAGE: All servers failed to respond
  ```

  This is a known issue from Cisco NX-OS Release 8.0(1) onwards and there is no workaround. If the remote authentication works properly without any TACACS server connectivity issue, you can ignore the message and continue with your further configuration.
- You can configure a maximum of 64 TACACS+ servers on the Cisco NX-OS device.
- If you have a user account configured on the local Cisco NX-OS device that has the same name as a remote user account on an AAA server, the Cisco NX-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.
- Cisco recommends that you configure the dead-time interval if more than six servers are configured in a group. If you must configure more than six servers, make sure to set the dead-time interval to a value greater than 0 and enable dead server monitoring by configuring the test username and test password.
- For Cisco NX-OS Releases 4.x and 5.x, command authorization on TACACS+ servers is available only for non-console sessions. If you use a console to login to the server, command authorization is disabled. Beginning with Cisco NX-OS Release 6.0, command authorization on TACACS+ servers is available for both console and non-console sessions.

Default Settings for TACACS+

This table lists the default settings for TACACS+ parameters.

Table 12: Default TACACS+ Parameters Settings

Parameters	Default
TACACS+	Disabled
Dead timer interval	0 minutes
Timeout interval	5 seconds
Idle timer interval	0 minutes
Periodic server monitoring username	test
Periodic server monitoring password	test
Privilege level support for TACACS+ authorization	Disabled

Configuring TACACS+

This section describes how to configure TACACS+ on a Cisco NX-OS device.

Note 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.

TACACS+ Server Configuration Process

Step 1 Enable TACACS+.
Step 2 If needed, enable CFS configuration distribution for TACACS+.
Step 3 Establish the TACACS+ server connections to the Cisco NX-OS device.
Step 4 Configure the secret keys for the TACACS+ servers.
Step 5 If needed, configure TACACS+ server groups with subsets of the TACACS+ servers for AAA authentication methods.
Step 6 (Optional) Configure the TCP port.
Step 7 (Optional) If needed, configure periodic TACACS+ server monitoring.
Step 8 (Optional) If TACACS+ distribution is enabled, commit the TACACS+ configuration to the fabric.

Related Topics

Enabling TACACS+ , on page 100

Enabling TACACS+

By default, the TACACS+ feature is disabled on the Cisco NX-OS device. You must explicitly enable the TACACS+ feature to access the configuration and verification commands for authentication.

SUMMARY STEPS

1. **configure terminal**
2. **feature tacacs+**
3. **exit**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**feature tacacs+** **Example:** `switch(config)# feature tacacs+`	Enables TACACS+.

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

Step 4	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring TACACS+ Server Hosts

To access a remote TACACS+ server, you must configure the IP address or the hostname for the TACACS+ server on the Cisco NX-OS device. You can configure up to 64 TACACS+ servers.

Note By default, when you configure a TACACS+ server IP address or hostname on the Cisco NX-OS device, the TACACS+ server is added to the default TACACS+ server group. You can also add the TACACS+ server to another TACACS+ server group.

Before you begin

Enable TACACS+.

Obtain the IPv4 or IPv6 addresses or the hostnames for the remote TACACS+ servers.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*host-name* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **6** | **7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*] [**single-connection**]
3. (Optional) **show tacacs+** {**pending** | **pending-diff**}
4. (Optional) **tacacs+ commit**
5. **exit**
6. (Optional) **show tacacs-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs-server host** {*host-name* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **6** | **7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*] [**single-connection**] **Example:** `switch(config)# tacacs-server host 10.10.2.2`	Specifies the IPv4 or IPv6 address or hostname for a TACACS+ server. Use the **single-connection** option to improve performance by configuring a single TACACS+ connection. Rather than have the device open and close a TCP connection to the daemon each time it must communicate, this option maintains a single open connection between the device and the daemon.
Step 3	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	Displays the TACACS+ configuration pending for distribution.
Step 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

	Command or Action	Purpose
Step 6	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	Displays the TACACS+ server configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling TACACS+ , on page 100
Enabling TACACS+ Configuration Distribution, on page 126
Configuring TACACS+ Server Groups, on page 105

Configuring Global TACACS+ Keys

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

Note CFS does not distribute the TACACS+ global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.

Before you begin

Enable TACACS+.

Obtain the secret key values for the remote TACACS+ servers.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server key** [**0** | **6** | **7**] *key-value*
3. **exit**
4. (Optional) **show tacacs-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 2	**tacacs-server key** [**0** | **6** | **7**] *key-value* **Example:** `switch(config)# tacacs-server key 0 QsEfThUkO`	Specifies a TACACS+ key for all TACACS+ server. You can specify that the *key-value* is in clear text format (**0**), is type-6 encrypted (**6**), or is type-7 encrypted (**7**). The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters. By default, no secret key is configured.

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

Step 4	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	Displays the TACACS+ server configuration. **Note** The secret keys are saved in encrypted form in the running configuration. Use the **show running-config** command to display the encrypted secret keys.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

AES Password Encryption and Master Encryption Keys, on page 30
Enabling TACACS+ , on page 100
Enabling TACACS+ Configuration Distribution, on page 126

Configuring a Key for a Specific TACACS+ Server

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

Note CFS does not distribute the TACACS+ server keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.

Before you begin

Enable TACACS+.

Obtain the secret key values for the remote TACACS+ servers.

SUMMARY STEPS

1. **configure terminal**

2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **6** | **7**] *key-value*
3. **exit**
4. (Optional) **show tacacs-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **6** | **7**] *key-value* **Example:** `switch(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg`	Specifies a secret key for a specific TACACS+ server. You can specify the format of the secret key with the option **key**: • **key 0** specifies that the *key-value* entered is in clear text format • **key 6** specifies that the *key-value* entered is in type-6 encrypted format • **key 7** specifies that the *key-value* entered is in type-7 encrypted format If no key is specified, NX-OS software assumes the *key-value* to be clear text and encrypts it using type-7 encryption before saving it to running configuration. The maximum length of *key-value* is 63 characters This secret key is used instead of the global secret key. **Note** Type-6 encryption is done using AES cipher and a user-defined master key. Without this master key, type-6 keys are unusable. The master key is defined by the user and is never displayed in the configuration. Type-6 passwords are more secure. Type-7 encryption is done using a weak cipher and an encryption key that is hardwired into the OS. Type-7 passwords configured on one device can be decrypted on any other device because the encryption/decryption key is contained within the OS.

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

Step 4	(Optional) **show tacacs-server**	Displays the TACACS+ server configuration.

	Command or Action	Purpose
	Example: `switch# show tacacs-server`	**Note** The secret keys are saved in encrypted form in the running configuration. Use the **show running-config** command to display the encrypted secret keys.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

AES Password Encryption and Master Encryption Keys, on page 30

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.

Note CFS does not distribute the TACACS+ server group configuration.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*host-name* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **6** | **7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*] [**single-connection**]
3. **aaa group server tacacs+** *group-name*
4. **server** {*ipv4-address* | *ipv6-address* | *host-name*}
5. **exit**
6. (Optional) **show tacacs-server groups**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**tacacs-server host** {*host-name* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **6** | **7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*] [**single-connection**]
	
	Example:
	`switch(config)# tacacs-server host 10.10.2.2`
	`switch(config-tacacs+)#`
		Specifies the IPv4 or IPv6 address or hostname for a TACACS+ server.
		
		Use the **single-connection** option to improve performance by configuring a single TACACS+ connection. Rather than have the device open and close a TCP connection to the daemon each time it must communicate, this option maintains a single open connection between the device and the daemon.

Step 3	**aaa group server tacacs+** *group-name*
	
	Example:
	`switch(config)# aaa group server tacacs+ TacServer`
	`switch(config-tacacs+)#`
		Creates a TACACS+ server group and enters the TACACS+ server group configuration mode for that group.

Step 4	**server** {*ipv4-address* | *ipv6-address* | *host-name*} **Example:** `switch(config-tacacs+)# server 10.10.2.2`	Configures the TACACS+ server as a member of the TACACS+ server group. If the specified TACACS+ server is not found, configure it using the **tacacs-server host** command and retry this command.

Step 5	**exit**
	
	Example:
	`switch(config-tacacs+)# exit`
	`switch(config)#`
		Exits TACACS+ server group configuration mode.

Step 6	(Optional) **show tacacs-server groups** **Example:** `switch(config)# show tacacs-server groups`	Displays the TACACS+ server group configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling TACACS+ , on page 100
Remote AAA Services, on page 27
Configuring TACACS+ Server Hosts, on page 100
Configuring the TACACS+ Dead-Time Interval, on page 116

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. By default, the Cisco NX-OS software uses any available interface.

SUMMARY STEPS

1. **configure terminal**
2. **ip tacacs source-interface** *interface*
3. **exit**
4. (Optional) **show tacacs-server**
5. (Optional) **copy running-config startup config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)`
		Enters global configuration mode.

Step 2	**ip tacacs source-interface** *interface* **Example:** `switch(config)# ip tacacs source-interface mgmt 0`	Configures the global source interface for all TACACS+ server groups configured on the device.

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

Step 4	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	Displays the TACACS+ server configuration information.
Step 5	(Optional) **copy running-config startup config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling TACACS+ , on page 100
Configuring TACACS+ Server Groups, on page 105

Allowing Users to Specify a TACACS+ Server at Login

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

Note If you enable the directed-request option, the Cisco NX-OS device uses only the TACACS+ method for authentication and not the default local method.

Note User-specified logins are supported only for Telnet sessions.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server directed-request**
3. (Optional) **show tacacs+** {**pending** | **pending-diff**}
4. (Optional) **tacacs+ commit**
5. **exit**
6. (Optional) **show tacacs-server directed-request**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs-server directed-request** **Example:** `switch(config)# tacacs-server directed-request`	Allows users to specify a TACACS+ server to send the authentication request when logging in. The default is disabled.
Step 3	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	Displays the pending TACACS+ configuration.
Step 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other NX-OS devices if you have enabled CFS configuration distribution for the user role feature.
Step 5	**exit** **Example:**	Exits configuration mode.

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	
Step 6	(Optional) **show tacacs-server directed-request** **Example:** `switch# show tacacs-server directed-request`	Displays the TACACS+ directed request configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling TACACS+ , on page 100
Enabling TACACS+ Configuration Distribution, on page 126

Configuring the Global TACACS+ Timeout Interval

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

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. From the Feature Selector pane, choose **Security** > **AAA** > **Server Groups**.
2. From the Summary pane, double-click the device to display the server groups.
3. Click **Default TACACS Server Group**.
4. From the Details pane, click the **Global Settings** tab.
5. In the Time out(secs) field, enter the number of seconds for the timeout interval.
6. From the menu bar, choose **File** > **Deploy** to apply your changes to the device.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Security** > **AAA** > **Server Groups**.

Step 2 From the Summary pane, double-click the device to display the server groups.

Step 3 Click **Default TACACS Server Group**.

Step 4 From the Details pane, click the **Global Settings** tab.

Step 5 In the Time out(secs) field, enter the number of seconds for the timeout interval.

The default is 5 seconds.

Step 6 From the menu bar, choose **File** > **Deploy** to apply your changes to the device.

Related Topics

Enabling TACACS+ , on page 100
Enabling TACACS+ Configuration Distribution, on page 126

Configuring the Timeout Interval for a TACACS+ Server

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

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout** *seconds*
3. (Optional) **show tacacs+** {**pending** | **pending-diff**}
4. (Optional) **tacacs+ commit**
5. **exit**
6. (Optional) **show tacacs-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout** *seconds* **Example:** `switch(config)# tacacs-server host server1 timeout 10`	Specifies the timeout interval for a specific server. The default is the global value. **Note** The timeout interval value specified for a TACACS+ server overrides the global timeout interval value specified for all TACACS+ servers.
Step 3	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	Displays the TACACS+ configuration pending for distribution.
Step 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes the TACACS+ configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

	Command or Action	Purpose

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 6	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	Displays the TACACS+ server configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling TACACS+ , on page 100
Enabling TACACS+ Configuration Distribution, on page 126

Configuring TCP Ports

You can configure another TCP port for the TACACS+ servers if there are conflicts with another application. By default, Cisco NX-OS devices use port 49 for all TACACS+ requests.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **port** *tcp-port*
3. (Optional) **show tacacs+** {**pending** | **pending-diff**}
4. (Optional) **tacacs+ commit**
5. **exit**
6. (Optional) **show tacacs-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 2	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **port** *tcp-port* **Example:** `switch(config)# tacacs-server host 10.10.1.1 port 2`	Specifies the TCP port to use for TACACS+ messages to the server. The default TCP port is 49. The range is from 1 to 65535.
Step 3	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ distribution pending`	Displays the TACACS+ configuration pending for distribution.
Step 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 6	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	Displays the TACACS+ server configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling TACACS+ , on page 100
Enabling TACACS+ Configuration Distribution, on page 126

Configuring Global Periodic TACACS+ Server Monitoring

You can monitor the availability of all TACACS+ servers without having to configure the test parameters for each server individually. Any servers for which test parameters are not configured are monitored using the global level parameters.

Note Test parameters that are configured for individual servers take precedence over global test parameters.

The global configuration parameters include the username and password to use for the servers and an idle timer. The idle timer specifies the interval in which a TACACS+ server receives no requests before the Cisco NX-OS 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 The test parameters are distributed across switches running Cisco NX-OS Release 5.x or later. If even one switch in the fabric is running an older release, the test parameters are not distributed to any switch in the fabric.

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.

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

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}
3. **tacacs-server dead-time** *minutes*
4. **exit**
5. (Optional) **show tacacs-server**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs-server test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **Example:** `switch(config)# tacacs-server test username user1 password Ur2Gd2BH idle-time 3`	Specifies parameters for global server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes. **Note** For periodic TACACS+ server monitoring, the idle timer value must be greater than 0.
Step 3	**tacacs-server dead-time** *minutes* **Example:**	Specifies the number of minutes before the Cisco NX-OS device checks a TACACS+ server that was previously

	Command or Action	Purpose
	`switch(config)# tacacs-server dead-time 5`	unresponsive. The default value is 0 minutes, and the valid range is from 0 to 1440 minutes.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	Displays the TACACS+ server configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring Periodic TACACS+ Server Monitoring on Individual Servers, on page 114

Configuring Periodic TACACS+ Server Monitoring on Individual Servers

You can monitor the availability of individual TACACS+ servers. The configuration 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 NX-OS 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 Test parameters that are configured for individual servers take precedence over global test parameters.

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.

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

Note The test parameters are distributed across switches running Cisco NX-OS Release 5.x. If even one switch in the fabric is running an older release, the test parameters are not distributed to any switch in the fabric.

Before you begin

Enable TACACS+.

Add one or more TACACS+ server hosts.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}
3. **tacacs-server dead-time** *minutes*
4. **exit**
5. (Optional) **show tacacs-server**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **Example:** `switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3`	Specifies parameters for individual server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes. **Note** For periodic TACACS+ server monitoring, the idle timer value must be greater than 0.
Step 3	**tacacs-server dead-time** *minutes* **Example:** `switch(config)# tacacs-server dead-time 5`	Specifies the number of minutes before the Cisco NX-OS device checks a TACACS+ server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 0 to 1440 minutes.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	Displays the TACACS+ server configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring TACACS+ Server Hosts, on page 100
Enabling TACACS+ Configuration Distribution, on page 126
Configuring Global Periodic TACACS+ Server Monitoring, on page 112

Configuring the TACACS+ Dead-Time Interval

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

Note

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

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server deadtime** *minutes*
3. (Optional) **show tacacs+** {**pending** | **pending-diff**}
4. (Optional) **tacacs+ commit**
5. **exit**
6. (Optional) **show tacacs-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs-server deadtime** *minutes* **Example:** `switch(config)# tacacs-server deadtime 5`	Configures the global dead-time interval. The default value is 0 minutes. The range is from 1 to 1440 minutes.
Step 3	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	Displays the pending TACACS+ configuration.

	Command or Action	Purpose
Step 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 6	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	Displays the TACACS+ server configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling TACACS+ Configuration Distribution, on page 126

Configuring ASCII Authentication

You can enable ASCII authentication on the TACACS+ server.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login ascii-authentication**
3. (Optional) **show tacacs+** {**pending** | **pending-diff**}
4. (Optional) **tacacs+ commit**
5. **exit**
6. (Optional) **show tacacs-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
Step 2	**aaa authentication login ascii-authentication** **Example:** `switch(config)# aaa authentication login ascii-authentication`	Enables ASCII authentication. The default is disabled.
Step 3	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	Displays the pending TACACS+ configuration.
Step 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to the other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 6	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	Displays the TACACS+ server configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring AAA Authorization on TACACS+ Servers

You can configure the default AAA authorization method for TACACS+ servers.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authorization ssh-certificate default** {**group** *group-list* [**none**] | **local** | **none**}
3. **exit**
4. (Optional) **show aaa authorization** [**all**]
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**aaa authorization ssh-certificate default** {**group** *group-list* [**none**] | **local** | **none**}
	Example:
	`switch(config)# aaa authorization ssh-certificate`
	`default group TACACSServer1 TACACSServer2`
		Configures the default AAA authorization method for the TACACS+ servers.
		The **ssh-certificate** keyword configures TACACS+ or local authorization with certificate authentication. The default authorization is local authorization, which is the list of authorized commands for the user's assigned role.
		The *group-list* argument consists of a space-delimited list of TACACS+ server group names. Servers belonging to this group are contacted for AAA authorization. The **local** method uses the local database for authorization, and the **none** method specifies that no AAA authorization be used.

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

Step 4	(Optional) **show aaa authorization** [**all**] **Example:** `switch# show aaa authorization`	Displays the AAA authorization configuration. The **all** keyword displays the default values.

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

Related Topics

Enabling TACACS+ , on page 100

Configuring Command Authorization on TACACS+ Servers

You can configure authorization for commands on TACACS+ servers.

Caution Command authorization disables user role-based authorization control (RBAC), including the default roles.

Note

- For Cisco NX-OS Releases 4.x and 5.x, command authorization is available only for non-console sessions. If you use a console to login to the server, command authorization is disabled. Beginning with Cisco NX-OS Release 6.0, command authorization is available for both non-console and console sessions. By default, command authorization is disabled for console sessions even if it is configured for default (non-console) sessions. You must explicitly configure a AAA group for the console to enable command authorization for console sessions.
- By default, context sensitive help and command tab completion show only the commands supported for a user as defined by the assigned roles. When you enable command authorization, the Cisco NX-OS software displays all commands in the context sensitive help and in tab completion, regardless of the role assigned to the user.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authorization** {**commands** | **config-commands**} {**console** | **default**}
3. (Optional) **show tacacs+** {**pending** | **pending-diff**}
4. (Optional) **tacacs+ commit**
5. **exit**
6. (Optional) **show aaa authorization** [**all**]
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**aaa authorization** {**commands** | **config-commands**} {**console** | **default**}
	Example:
	`switch(config)# aaa authorization commands`
	`default group TacGroup`
	`Per command authorization will disable RBAC for`
	`all`
	`users. Proceed (y/n)?`
		Configures the command authorization method for specific roles on a TACACS+ server.
		The **commands** keyword configures authorization sources for all EXEC commands, and the **config-commands** keyword configures authorization sources for all configuration commands.
		The **console** keyword configures command authorization for a console session, and the **default** keyword configures command authorization for a non-console session.
		The *group-list* argument consists of a space-delimited list of TACACS+ server group names. Servers belonging to this group are contacted for command authorization. The

	Command or Action	Purpose
		local method uses the local role-based database for authorization. The **local** method is used only if all the configured server groups fail to respond and you have configured **local** as the fallback method. The default method is **local**. If you have not configured a fallback method after the TACACS+ server group method, authorization fails if all server groups fail to respond. If you press **Enter** at the confirmation prompt, the default action is `n`.
Step 3	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	Displays the pending TACACS+ configuration.
Step 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes TACACS+ configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 6	(Optional) **show aaa authorization** [**all**] **Example:** `switch(config)# show aaa authorization`	Displays the AAA authorization configuration. The **all** keyword displays the default values.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling TACACS+ , on page 100
Testing Command Authorization on TACACS+ Servers, on page 121

Testing Command Authorization on TACACS+ Servers

You can test the command authorization for a user on the TACACS+ servers.

Note You must send correct commands for authorization or else the results may not be reliable.

Note The **test** command uses the default (non-console) method for authorization, not the console method.

Before you begin

Enable TACACS+.

Ensure that you have configured command authorization for the TACACS+ servers.

SUMMARY STEPS

1. **test aaa authorization command-type** {**commands** | **config-commands**} **user** *username* **command** *command-string*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**test aaa authorization command-type** {**commands** | **config-commands**} **user** *username* **command** *command-string*
	Example:
	`switch# test aaa authorization command-type commands`
	`user TestUser command reload`
		Tests a user's authorization for a command on the TACACS+ servers.
		The **commands** keyword specifies only EXEC commands and the **config-commands** keyword specifies only configuration commands.
		Note Put double quotes (") before and after the *command-string* argument if it contains spaces.

Related Topics

Enabling TACACS+ , on page 100
Configuring Command Authorization on TACACS+ Servers, on page 119
Configuring User Accounts and RBAC, on page 235

Enabling and Disabling Command Authorization Verification

You can enable and disable command authorization verificaiton on the command-line interface (CLI) for the default user session or for another username.

Note The commands do no execute when you enable authorization verification.

SUMMARY STEPS

1. **terminal verify-only** [**username** *username*]
2. **terminal no verify-only** [**username** *username*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal verify-only** [**username** *username*] **Example:** `switch# terminal verify-only`	Enables command authorization verification. After you enter this command, the Cisco NX-OS software indicates whether the commands you enter are authorized or not.
Step 2	**terminal no verify-only** [**username** *username*] **Example:** `switch# terminal no verify-only`	Disables command authorization verification.

Configuring Privilege Level Support for Authorization on TACACS+ Servers

You can configure privilege level support for authorization on TACACS+ servers.

Unlike Cisco IOS devices, which use privilege levels to determine authorization, Cisco NX-OS devices use role-based access control (RBAC). To enable both types of devices to be administered by the same TACACS+ servers, you can map the privilege levels configured on TACACS+ servers to user roles configured on Cisco NX-OS devices.

When a user authenticates with a TACACS+ server, the privilege level is obtained and used to form a local user role name of the format "priv-*n*," where *n* is the privilege level. The user assumes the permissions of this local role. Sixteen privilege levels, which map directly to corresponding user roles, are available. The following table shows the user role permissions that correspond to each privilege level.

Privilege Level	User Role Permissions
15	network-admin permissions
14	vdc-admin permissions
13 - 1	• Standalone role permissions, if the **feature privilege** command is disabled. • Same permissions as privilege level 0 with cumulative privileges for roles, if the **feature privilege** command is enabled.
0	Permission to execute **show** commands and **exec** commands (such as **ping**, **trace**, and **ssh**).

Note When the **feature privilege** command is enabled, privilege roles inherit the permissions of lower level privilege roles.

Note You must also configure the privilege level for the Cisco NX-OS device on the Cisco Secure Access Control Server (ACS). See the documentation at the following URL:

http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_installation_and_configuration_guides_list.html

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **feature privilege**
3. [**no**] **enable secret** [**0** | **5**] *password* [**priv-lvl** *priv-lvl* | **all**]
4. [**no**] **username** *username* **priv-lvl** *n*
5. (Optional) **show privilege**
6. (Optional) **copy running-config startup-config**
7. **exit**
8. **enable** *level*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **feature privilege** **Example:** `switch(config)# feature privilege`	Enables or disables the cumulative privilege of roles. Users can see the **enable** command only if this feature is enabled. The default is disabled.
Step 3	[**no**] **enable secret** [**0** | **5**] *password* [**priv-lvl** *priv-lvl* | **all**] **Example:** `switch(config)# enable secret 5 def456 priv-lvl 15`	Enables or disables a secret password for a specific privilege level. Users are prompted to enter the correct password upon each privilege level escalation. The default is disabled. You can enter **0** to specify that the password is in clear text or **5** to specify that the password is in encrypted format. The *password* argument can be up to 64 alphanumeric characters. The *priv-lvl* argument is from 1 to 15. **Note** To enable the secret password, you must have enabled the cumulative privilege of roles by entering the **feature privilege** command.
Step 4	[**no**] **username** *username* **priv-lvl** *n* **Example:** `switch(config)# username user2 priv-lvl 15`	Enables or disables a user to use privilege levels for authorization. The default is disabled. The **priv-lvl** keyword specifies the privilege level to which the user is assigned. There is no default privilege level. Privilege levels 0 to 15 (priv-lvl 0 to priv-lvl 15) map to user roles priv-0 to priv-15.

	Command or Action	Purpose
Step 5	(Optional) **show privilege** **Example:** `switch(config)# show privilege`	Displays the username, current privilege level, and status of cumulative privilege support.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Step 7	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 8	**enable** *level* **Example:** `switch# enable 15`	Enables a user to move to a higher privilege level. This command prompts for the secret password. The *level* argument specifies the privilege level to which the user is granted access. The only available level is 15.

Related Topics

Permitting or Denying Commands for Users of Privilege Roles, on page 125
Creating User Roles and Rules, on page 245

Permitting or Denying Commands for Users of Privilege Roles

As a network administrator, you can modify the privilege roles to permit users to execute specific commands or to prevent users from running those commands.

You must follow these guidelines when changing the rules of privilege roles:

- You cannot modify the priv-14 and priv-15 roles.
- You can add deny rules only to the priv-0 role.
- These commands are always permitted for the priv-0 role: **configure**, **copy**, **dir**, **enable**, **ping**, **show**, **ssh**, **telnet**, **terminal**, **traceroute**, **end**, and **exit**.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **role name priv-***n*
3. **rule** *number* {**deny** | **permit**} **command** *command-string*
4. **exit**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **role name priv-***n*
	Example:
	`switch(config)# role name priv-5`
	`switch(config-role)#`
		Enables or disables a privilege role and enters role configuration mode. The *n* argument specifies the privilege level and is a number between 0 and 13.

Step 3	**rule** *number* {**deny** | **permit**} **command** *command-string* **Example:** `switch(config-role)# rule 2 permit command pwd`	Configures a command rule for users of privilege roles. These rules permit or deny users to execute specific commands. You can configure up to 256 rules for each role. The rule number determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1. The *command-string* argument can contain spaces. **Note** Repeat this command for as many rules as needed.

Step 4	**exit**
	Example:
	`switch(config-role)# exit`
	`switch(config)#`
		Exits role configuration mode.

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

Related Topics

Configuring Privilege Level Support for Authorization on TACACS+ Servers, on page 123
Creating User Roles and Rules, on page 245

Enabling TACACS+ Configuration Distribution

Only Cisco NX-OS devices that have distribution enabled can participate in the distribution of the TACACS+ configuration changes in the CFS region.

Before you begin

Ensure that CFS distribution is enabled.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs+ distribute**
3. **exit**
4. (Optional) **show tacacs+ status**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**tacacs+ distribute** **Example:** `switch(config)# tacacs+ distribute`	Enables TACACS+ configuration distribution. The default is disabled.

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

Step 4	(Optional) **show tacacs+ status** **Example:** `switch(config)# show tacacs+ status`	Displays the TACACS+ CFS distribution configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling TACACS+ , on page 100
Configuring TACACS+ Server Hosts, on page 100
TACACS+ Server Configuration Process, on page 99
Configuring TACACS+ Server Groups, on page 105

Committing the TACACS+ Configuration to Distribution

You can apply the TACACS+ global and server configuration stored in the temporary buffer to the running configuration across all Cisco NX-OS devices in the fabric (including the originating device).

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **show tacacs+** {**pending** | **pending-diff**}
3. **tacacs+ commit**
4. **exit**
5. (Optional) **show tacacs+ distribution status**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	Displays the TACACS+ configuration pending for distribution.
Step 3	**tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	Applies the TACACS+ configuration changes in the temporary database to the running configuration and distributes the TACACS+ configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show tacacs+ distribution status** **Example:** `switch(config)# show tacacs+ distribution status`	Displays the TACACS distribution configuration and status.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Applies the running configuration to the startup configuration.

Related Topics

Enabling TACACS+ Configuration Distribution, on page 126

Discarding the TACACS+ Distribution Session

You can discard the temporary database of TACACS+ changes and end the CFS distribution session.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **show tacacs+** {**pending** | **pending-diff**}
3. **tacacs+ abort**
4. **exit**
5. (Optional) **show tacacs+ distribution status**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	Displays the TACACS+ configuration pending for distribution.
Step 3	**tacacs+ abort** **Example:** `switch(config)# tacacs+ abort`	Discards the TACACS+ configuration in the temporary storage and ends the session.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show tacacs+ distribution status** **Example:** `switch(config)# show tacacs+ distribution status`	Displays the TACACS distribution configuration and status.

Related Topics

Enabling TACACS+ Configuration Distribution, on page 126

Clearing the TACACS+ Distribution Session

You can clear an active CFS distribution session and unlock TACACS+ configuration in the network.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **clear tacacs+ session**
2. (Optional) **show tacacs+ distribution status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clear tacacs+ session** **Example:** `switch# clear tacacs+ session`	Clears the CFS session for TACACS+ and unlocks the fabric.
Step 2	(Optional) **show tacacs+ distribution status** **Example:** `switch(config)# show tacacs+ distribution status`	Displays the TACACS distribution configuration and status.

Related Topics

Enabling TACACS+ Configuration Distribution, on page 126

Manually Monitoring TACACS+ Servers or Groups

You can manually issue a test message to a TACACS+ server or to a server group.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **test aaa server tacacs+** {*ipv4-address* | *ipv6-address* | *host-name*} [**vrf** *vrf-name*] *username password*
2. **test aaa group** *group-name username password*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**test aaa server tacacs+** {*ipv4-address* | *ipv6-address* | *host-name*} [**vrf** *vrf-name*] *username password* **Example:** `switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH`	Sends a test message to a TACACS+ server to confirm availability.
Step 2	**test aaa group** *group-name username password* **Example:** `switch# test aaa group TacGroup user2 As3He3CI`	Sends a test message to a TACACS+ server group to confirm availability.

Related Topics

Configuring TACACS+ Server Hosts, on page 100

Configuring TACACS+ Server Groups, on page 105

Disabling TACACS+

You can disable TACACS+.

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

SUMMARY STEPS

1. **configure terminal**
2. **no feature tacacs+**
3. **exit**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no feature tacacs+** **Example:** `switch(config)# no feature tacacs+`	Disables TACACS+.

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

Step 4	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Monitoring TACACS+ Servers

You can monitor the statistics that the Cisco NX-OS device maintains for TACACS+ server activity.

Before you begin

Configure TACACS+ servers on the Cisco NX-OS device.

SUMMARY STEPS

1. **show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} **Example:** `switch# show tacacs-server statistics 10.10.1.1`	Displays the TACACS+ statistics.

Related Topics

Configuring TACACS+ Server Hosts, on page 100
Clearing TACACS+ Server Statistics, on page 132

Clearing TACACS+ Server Statistics

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

Before you begin

Configure TACACS+ servers on the Cisco NX-OS device.

SUMMARY STEPS

1. (Optional) **show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}
2. **clear tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} **Example:** `switch# show tacacs-server statistics 10.10.1.1`	Displays the TACACS+ server statistics on the Cisco NX-OS device.
Step 2	**clear tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} **Example:** `switch# clear tacacs-server statistics 10.10.1.1`	Clears the TACACS+ server statistics.

Related Topics

Configuring TACACS+ Server Hosts, on page 100

Verifying the TACACS+ Configuration

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

Command	Purpose
show tacacs+ { **status** | **pending** | **pending-diff**}	Displays the TACACS+ Cisco Fabric Services distribution status and other details.
show running-config tacacs+ [**all**]	Displays the TACACS+ configuration in the running configuration.
show startup-config tacacs	Displays the TACACS+ configuration in the startup configuration.
show tacacs-server [*host-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	Displays all configured TACACS+ server parameters.
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.

For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuration Examples for TACACS+

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

```
feature tacacs+
tacacs-server key 7 "ToIkLhPpG"
tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
aaa group server tacacs+ TacServer
    server 10.10.2.2
```

The following example shows how to configure and use command authorization verification:

```
switch# terminal verify-only
switch# show interface ethernet 7/2 brief
%Success
switch# terminal no verify-only
switch# show interface ethernet 7/2 brief

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                   Ch #
--------------------------------------------------------------------------------
Eth7/2        1      eth  access down    SFP not inserted           auto(D) --
```

The following example shows how to enable the cumulative privilege of roles, configure a secret password for privilege level 2, and configure user3 for privilege level 2 authorization:

```
switch# configure terminal
switch(config)# feature privilege
switch(config)# enable secret def456 priv-lvl 2
switch(config)# username user3 priv-lvl 2
switch(config)# show privilege
User name: user3
Current privilege level: -2
Feature privilege: Enabled
switch(config)# copy running-config startup-config
switch(config)# exit
```

The following example shows how to change user3 from the priv-2 role to the priv-15 role. After entering the **enable 15** command, the user is prompted to enter the password that was configured by the administrator using the **enable secret** command. Privilege level 15 gives this user network-admin privileges under the enable mode.

```
User Access Verification
login: user3
Password: ******
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright ©) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch#
switch# enable 15
Password: def456
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright ©) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch-enable#
```

The following example shows how to permit all users with roles priv-5 and above to execute the **pwd** command:

```
switch# configure terminal
switch(config)# role name priv-5
switch(config-role)# rule 1 permit command pwd
```

The following example shows how to deny the **show running-config** command to all users with roles below priv-5. First, you must remove the permission to execute this command from the priv-0 role; then you must permit the command at role priv-5 so that users with roles priv-5 and above have permission to run the command.

```
switch# configure terminal
switch(config)# role name priv-0
switch(config-role)# rule 2 deny command show running-config
switch(config-role)# exit
switch(config)# role name priv-5
switch(config-role)# rule 3 permit command show running-config
switch(config-role)# exit
```

Where to Go Next

You can now configure AAA authentication methods to include the server groups.

Additional References for TACACS+

This section includes additional information related to implementing TACACS+.

Related Documents

Related Topic	Document Title
Cisco NX-OS licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
VRF configuration	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

- CISCO-AAA-SERVER-MIB
- CISCO-AAA-SERVER-EXT-MIB

Feature History for TACACS+

This table lists the release history for this feature.

Table 13: Feature History for TACACS+

Feature Name	Releases	Feature Information
TACACS+	6.2(2)	Added support for a single TACACS+ connection.
TACACS+	6.0(1)	Added the ability to configure command authorization for a console session.
TACACS+	5.2(1)	Added type-6 encryption for TACACS+ server keys.
TACACS+	5.1(1)	No change from Release 5.0.
TACACS+ privilege-level authorization	5.0(2)	Added support for the mapping of privilege levels configured for users on the TACACS+ server to locally configured user roles on the Cisco NX-OS device.
Privilege roles	5.0(2)	Added support for permitting or denying commands for users of privilege roles.
Periodic server monitoring	5.0(2)	Added support for global periodic TACACS+ server monitoring.
AAA authorization	5.0(2)	Added support for configuring the default AAA authorization method for TACACS+ servers.

CHAPTER 7

Configuring LDAP

This chapter describes how to configure the Lightweight Directory Access Protocol (LDAP) on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About LDAP

The Lightweight Directory Access Protocol (LDAP) provides centralized validation of users attempting to gain access to a Cisco NX-OS device. LDAP services are maintained in a database on an LDAP daemon running, typically, on a UNIX or Windows NT workstation. You must have access to and must configure an LDAP server before the configured LDAP features on your Cisco NX-OS device are available.

LDAP provides for separate authentication and authorization facilities. LDAP allows for a single access control server (the LDAP daemon) to provide each service—authentication and authorization—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The LDAP client/server protocol uses TCP (TCP port 389) for transport requirements. Cisco NX-OS devices provide centralized authentication using the LDAP protocol.

LDAP Authentication and Authorization

Clients establish a TCP connection and authentication session with an LDAP server through a simple bind (username and password). As part of the authorization process, the LDAP server searches its database to retrieve the user profile and other information.

You can configure the bind operation to first bind and then search, where authentication is performed first and authorization next, or to first search and then bind. The default method is to first search and then bind.

The advantage of searching first and binding later is that the distinguished name (DN) received in the search result can be used as the user DN during binding rather than forming a DN by prepending the username (cn attribute) with the baseDN. This method is especially helpful when the user DN is different from the username plus the baseDN. For the user bind, the bindDN is constructed as baseDN + append-with-baseDN, where append-with-baseDN has a default value of cn=$userid.

Note As an alternative to the bind method, you can establish LDAP authentication using the compare method, which compares the attribute values of a user entry at the server. For example, the user password attribute can be compared for authentication. The default password attribute type is userPassword.

LDAP Operation for User Login

When a user attempts a Password Authentication Protocol (PAP) login to a Cisco NX-OS device using LDAP, the following actions occur:

Note LDAP 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.

Note In LDAP, authorization can occur before authentication.

1. When the Cisco NX-OS device establishes a connection, it contacts the LDAP daemon to obtain the username and password.
2. The Cisco NX-OS device eventually receives one of the following responses from the LDAP daemon:

   ACCEPT
   User authentication succeeds and service begins. If the Cisco NX-OS device requires user authorization, authorization begins.

REJECT
User authentication fails. The LDAP daemon either denies further access to the user or prompts the user to retry the login sequence.
ERROR
An error occurs at some time during authentication either at the daemon or in the network connection between the daemon and the Cisco NX-OS device. If the Cisco NX-OS device receives an ERROR response, the Cisco NX-OS device tries to use an alternative method for authenticating the user.

After authentication, the user also undergoes an additional authorization phase if authorization has been enabled on the Cisco NX-OS device. Users must first successfully complete LDAP authentication before proceeding to LDAP authorization.

3. If LDAP authorization is required, the Cisco NX-OS device again contacts the LDAP 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:

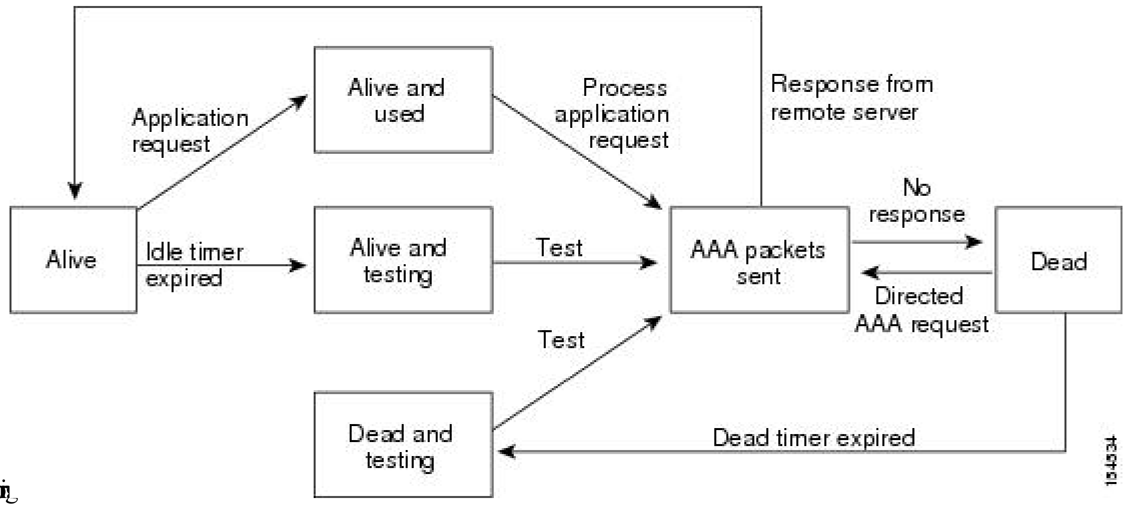
   - Telnet, rlogin, Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services
   - Connection parameters, including the host or client IP address (IPv4 or IPv6), access list, and user timeouts

LDAP Server Monitoring

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

Figure 4: LDAP Server States

This figure shows the server states for LDAP server



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

Vendor-Specific Attributes for LDAP

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific attributes (VSAs) between the network access server and the LDAP server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use.

Cisco VSA Format for LDAP

The Cisco LDAP implementation supports one vendor-specific option using the format recommended in the IETF 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 = (equal sign) for mandatory attributes, and * (asterisk) indicates optional attributes.

When you use LDAP servers for authentication on a Cisco NX-OS device, LDAP directs the LDAP server to return user attributes, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

The following VSA protocol options are supported by the Cisco NX-OS software:

Shell
: Protocol used in access-accept packets to provide user profile information.

The Cisco NX-OS software 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 space. For example, if the user belongs to roles network-operator and vdc-admin, the value field would be network-operator vdc-admin. This subattribute, which the LDAP server sends in the VSA portion of the Access-Accept frames, can only be used with the shell protocol value. The following examples show the roles attribute as supported by Cisco ACS:

```
shell:roles=network-operator vdc-admin
```

```
shell:roles*network-operator vdc-admin
```

Note When you specify a VSA as shell:roles*"network-operator vdc-admin", this VSA is flagged as an optional attribute and other Cisco devices ignore this attribute.

Virtualization Support for LDAP

LDAP configuration and operation are local to the virtual device context (VDC). For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

The Cisco NX-OS device uses virtual routing and forwarding instances (VRFs) to access the LDAP servers. For more information on VRFs, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

Prerequisites for LDAP

LDAP has the following prerequisites:

- Obtain the IPv4 or IPv6 addresses or hostnames for the LDAP servers.
- Ensure that the Cisco NX-OS device is configured as an LDAP client of the AAA servers.

Guidelines and Limitations for LDAP

LDAP has the following guidelines and limitations:

- You can configure a maximum of 64 LDAP servers on the Cisco NX-OS device.
- Cisco NX-OS supports only LDAP version 3.
- Cisco NX-OS supports only these LDAP servers:
    - OpenLDAP
    - Microsoft Active Directory
- LDAP over Secure Sockets Layer (SSL) supports only SSL version 3 and Transport Layer Security (TLS) version 1.

- If you have a user account configured on the local Cisco NX-OS device that has the same name as a remote user account on an AAA server, the Cisco NX-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.

Default Settings for LDAP

This table lists the default settings for LDAP parameters.

Table 14: Default LDAP Parameters Settings

Parameters	Default
LDAP	Disabled
LDAP authentication method	First search and then bind
LDAP authentication mechanism	Plain
Dead-time interval	0 minutes
Timeout interval	5 seconds
Idle timer interval	60 minutes
Periodic server monitoring username	test
Periodic server monitoring password	Cisco

Configuring LDAP

This section describes how to configure LDAP on a Cisco NX-OS device.

Note 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.

LDAP Server Configuration Process

You can configure LDAP servers by following this configuration process.

Step 1 Enable LDAP.

Step 2 Establish the LDAP server connections to the Cisco NX-OS device.

Step 3 If needed, configure LDAP server groups with subsets of the LDAP servers for AAA authentication methods.

Step 4 (Optional) Configure the TCP port.

Step 5 (Optional) Configure the default AAA authorization method for the LDAP server.

Step 6 (Optional) Configure an LDAP search map.

Step 7 (Optional) If needed, configure periodic LDAP server monitoring.

Related Topics

Enabling LDAP, on page 143
Configuring LDAP Server Hosts, on page 144
Configuring the RootDN for an LDAP Server, on page 145
Configuring LDAP Server Groups, on page 146
Configuring TCP Ports, on page 151
Configuring LDAP Search Maps, on page 152
Configuring Periodic LDAP Server Monitoring, on page 153

Enabling LDAP

By default, the LDAP feature is disabled on the Cisco NX-OS device. You must explicitly enable the LDAP feature to access the configuration and verification commands for authentication.

SUMMARY STEPS

1. **configure terminal**
2. **feature ldap**
3. **exit**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**feature ldap** **Example:** `switch(config)# feature ldap`	Enables LDAP.

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

Step 4	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring LDAP Server Hosts

To access a remote LDAP server, you must configure the IP address or the hostname for the LDAP server on the Cisco NX-OS device. You can configure up to 64 LDAP servers.

Note By default, when you configure an LDAP server IP address or hostname on the Cisco NX-OS device, the LDAP server is added to the default LDAP server group. You can also add the LDAP server to another LDAP server group.

Before you begin

Enable LDAP.

Obtain the IPv4 or IPv6 addresses or the hostnames for the remote LDAP servers.

If you plan to enable the Secure Sockets Layer (SSL) protocol, make sure that the LDAP server certificate is manually configured on the Cisco NX-OS device.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} [**enable-ssl**]
3. **exit**
4. (Optional) **show ldap-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} [**enable-ssl**] **Example:** `switch(config)# ldap-server host 10.10.2.2 enable-ssl`	Specifies the IPv4 or IPv6 address or hostname for an LDAP server. The **enable-ssl** keyword ensures the integrity and confidentiality of the transferred data by causing the LDAP client to establish a Secure Sockets Layer (SSL) session prior to sending the bind or search request.

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

Step 4	(Optional) **show ldap-server** **Example:**	Displays the LDAP server configuration.

	Command or Action	Purpose
	`switch# show ldap-server`	
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling LDAP, on page 143
Configuring LDAP Server Groups, on page 146

Configuring the RootDN for an LDAP Server

You can configure the root designated name (DN) for the LDAP server database. The rootDN is used to bind to the LDAP server to verify its state.

Before you begin

Enable LDAP.

Obtain the IPv4 or IPv6 addresses or the hostnames for the remote LDAP servers.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **rootDN** *root-name* [**password** *password*] [**port** *tcp-port* [**timeout** *seconds*] | [**timeout** *seconds*]]
3. **exit**
4. (Optional) **show ldap-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **rootDN** *root-name* [**password** *password*] [**port** *tcp-port* [**timeout** *seconds*] | [**timeout** *seconds*]] **Example:** `switch(config)# ldap-server host 10.10.1.1 rootDN cn=manager,dc=acme,dc=com password Ur2Gd2BH timeout 60`	Specifies the rootDN for the LDAP server database and the bind password for the root. Optionally specifies the TCP port to use for LDAP messages to the server. The range is from 1 to 65535, and the default TCP port is the global value or 389 if a global value is not configured. Also specifies the timeout interval for the server. The range is from 1 to 60 seconds, and the default timeout is the global value or 5 seconds if a global value is not configured.

	Command or Action	Purpose

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

Step 4	(Optional) **show ldap-server** **Example:** `switch# show ldap-server`	Displays the LDAP server configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling LDAP, on page 143
Configuring LDAP Server Hosts, on page 144

Configuring LDAP Server Groups

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

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

Before you begin

Enable LDAP.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **aaa group server ldap** *group-name*
3. [**no**] **server** {*ipv4-address* | *ipv6-address* | *host-name*}
4. (Optional) [**no**] **authentication** {**bind-first** [**append-with-baseDN** *DNstring*] | **compare** [**password-attribute** *password*]}
5. (Optional) [**no**] **enable user-server-group**
6. (Optional) [**no**] **enable Cert-DN-match**
7. (Optional) [**no**] **use-vrf** *vrf-name*
8. **exit**
9. (Optional) **show ldap-server groups**
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **aaa group server ldap** *group-name*
	Example:
	`switch(config)# aaa group server ldap LDAPServer1`
	`switch(config-ldap)#`
		Creates an LDAP server group and enters the LDAP server group configuration mode for that group.

Step 3	[**no**] **server** {*ipv4-address* | *ipv6-address* | *host-name*} **Example:** `switch(config-ldap)# server 10.10.2.2`	Configures the LDAP server as a member of the LDAP server group. If the specified LDAP server is not found, configure it using the **ldap-server host** command and retry this command.
Step 4	(Optional) [**no**] **authentication** {**bind-first** [**append-with-baseDN** *DNstring*] | **compare** [**password-attribute** *password*]} **Example:** `switch(config-ldap)# authentication compare password-attribute TyuL8r`	Performs LDAP authentication using the bind or compare method. The default LDAP authentication method is the bind method using first search and then bind.
Step 5	(Optional) [**no**] **enable user-server-group** **Example:** `switch(config-ldap)# enable user-server-group`	Enables group validation. The group name should be configured in the LDAP server. Users can login through public-key authentication only if the username is listed as a member of this configured group in the LDAP server.
Step 6	(Optional) [**no**] **enable Cert-DN-match** **Example:** `switch(config-ldap)# enable Cert-DN-match`	Enables users to login only if the user profile lists the subject-DN of the user certificate as authorized for login.
Step 7	(Optional) [**no**] **use-vrf** *vrf-name* **Example:** `switch(config-ldap)# use-vrf vrf1`	Specifies the VRF to use to contact the servers in the server group. **Note** This command is supported only on Cisco Nexus 7000 Series Switches.

Step 8	**exit**
	Example:
	`switch(config-ldap)# exit`
	`switch(config)#`
		Exits LDAP server group configuration mode.

Step 9	(Optional) **show ldap-server groups** **Example:** `switch(config)# show ldap-server groups`	Displays the LDAP server group configuration.

	Command or Action	Purpose
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling LDAP, on page 143
Configuring LDAP Server Hosts, on page 144

Configuring the Global LDAP Timeout Interval

You can set a global timeout interval that determines how long the Cisco NX-OS device waits for responses from all LDAP servers before declaring a timeout failure.

Before you begin

Enable LDAP.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ldap-server timeout** *seconds*
3. **exit**
4. (Optional) **show ldap-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ldap-server timeout** *seconds* **Example:** `switch(config)# ldap-server timeout 10`	Specifies the timeout interval for LDAP servers. The default timeout interval is 5 seconds. The range is from 1 to 60 seconds.

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

Step 4	(Optional) **show ldap-server** **Example:** `switch# show ldap-server`	Displays the LDAP server configuration.

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

Related Topics

Enabling LDAP, on page 143
Configuring the Timeout Interval for an LDAP Server, on page 149

Configuring the Timeout Interval for an LDAP Server

You can set a timeout interval that determines how long the Cisco NX-OS device waits for responses from an LDAP server before declaring a timeout failure.

Before you begin

Enable LDAP.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout** *seconds*
3. **exit**
4. (Optional) **show ldap-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout** *seconds* **Example:** `switch(config)# ldap-server host server1 timeout 10`	Specifies the timeout interval for a specific server. The default is the global value. **Note** The timeout interval value specified for an LDAP server overrides the global timeout interval value specified for all LDAP servers.

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

	Command or Action	Purpose
Step 4	(Optional) **show ldap-server** **Example:** `switch# show ldap-server`	Displays the LDAP server configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling LDAP, on page 143
Configuring the Global LDAP Timeout Interval, on page 148

Configuring the Global LDAP Server Port

You can configure a global LDAP server port through which clients initiate TCP connections. By default, Cisco NX-OS devices use port 389 for all LDAP requests.

Before you begin

Enable LDAP.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ldap-server port** *tcp-port*
3. **exit**
4. (Optional) **show ldap-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ldap-server port** *tcp-port* **Example:** `switch(config)# ldap-server port 2`	Specifies the global TCP port to use for LDAP messages to the server. The default TCP port is 389. The range is from 1 to 65535. **Note** This command is deprecated beginning with Cisco NX-OS Release 5.2.
Step 3	**exit** **Example:**	Exits configuration mode.

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	
Step 4	(Optional) **show ldap-server** **Example:** `switch# show ldap-server`	Displays the LDAP server configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling LDAP, on page 143
Configuring TCP Ports, on page 151

Configuring TCP Ports

You can configure another TCP port for the LDAP servers if there are conflicts with another application. By default, Cisco NX-OS devices use port 389 for all LDAP requests.

Before you begin

Enable LDAP.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **port** *tcp-port* [**timeout** *seconds*]
3. **exit**
4. (Optional) **show ldap-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **port** *tcp-port* [**timeout** *seconds*] **Example:** `switch(config)# ldap-server host 10.10.1.1 port 200 timeout 5`	Specifies the TCP port to use for LDAP messages to the server. The default TCP port is 389. The range is from 1 to 65535. Optionally specifies the timeout interval for the server. The range is from 1 to 60 seconds, and the default timeout is the global value or 5 seconds if a global value is not configured.

	Command or Action	Purpose
		Note The timeout interval value specified for an LDAP server overrides the global timeout interval value specified for all LDAP servers.

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

Step 4	(Optional) **show ldap-server** **Example:** `switch# show ldap-server`	Displays the LDAP server configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling LDAP, on page 143
Configuring the Global LDAP Server Port, on page 150

Configuring LDAP Search Maps

You can configure LDAP search maps to send a search query to the LDAP server. The server searches its database for data meeting the criteria specified in the search map.

Before you begin

Enable LDAP.

SUMMARY STEPS

1. **configure terminal**
2. **ldap search-map** *map-name*
3. (Optional) [**userprofile** | **trustedCert** | **CRLLookup** | **user-certdn-match** | **user-pubkey-match** | **user-switch-bind**] **attribute-name** *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name*
4. **exit**
5. (Optional) **show ldap-search-map**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**ldap search-map** *map-name*
	Example:
	`switch(config)# ldap search-map map1`
	`switch(config-ldap-search-map)#`
		Configures an LDAP search map.

Step 3	(Optional) [**userprofile** | **trustedCert** | **CRLLookup** | **user-certdn-match** | **user-pubkey-match** | **user-switch-bind**] **attribute-name** *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name* **Example:** `switch(config-ldap-search-map)# userprofile attribute-name att-name search-filter (&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com`	Configures the attribute name, search filter, and base-DN for the user profile, trusted certificate, CRL, certificate DN match, public key match, or user-switchgroup lookup search operation. These values are used to send a search query to the LDAP server. The *attribute-name* argument is the name of the attribute in the LDAP server that contains the Nexus role definition.

Step 4	**exit**
	Example:
	`switch(config-ldap-search-map)# exit`
	`switch(config)#`
		Exits LDAP search map configuration mode.

Step 5	(Optional) **show ldap-search-map** **Example:** `switch(config)# show ldap-search-map`	Displays the configured LDAP search maps.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling LDAP, on page 143

Configuring Periodic LDAP Server Monitoring

You can monitor the availability of LDAP servers. The configuration parameters include the username and password to use for the server, the rootDN to bind to the server to verify its state, and an idle timer. The idle timer specifies the interval in which an LDAP server receives no requests before the Cisco NX-OS 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 LDAP database.

Before you begin

Enable LDAP.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test rootDN** *root-name* [**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]]
3. [**no**] **ldap-server deadtime** *minutes*
4. **exit**
5. (Optional) **show ldap-server**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test rootDN** *root-name* [**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]] **Example:** `switch(config)# ldap-server host 10.10.1.1 test rootDN root1 username user1 password Ur2Gd2BH idle-time 3`	Specifies the parameters for server monitoring. The default username is test, and the default password is Cisco. The default value for the idle timer is 60 minutes, and the valid range is from 1 to 1440 minutes. **Note** We recommend that the user not be an existing user in the LDAP server database.
Step 3	[**no**] **ldap-server deadtime** *minutes* **Example:** `switch(config)# ldap-server deadtime 5`	Specifies the number of minutes before the Cisco NX-OS device checks an LDAP server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 1 to 60 minutes.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show ldap-server** **Example:** `switch# show ldap-server`	Displays the LDAP server configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling LDAP, on page 143
Configuring LDAP Server Hosts, on page 144

Configuring the LDAP Dead-Time Interval

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

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

Before you begin

Enable LDAP.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ldap-server deadtime** *minutes*
3. **exit**
4. (Optional) **show ldap-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ldap-server deadtime** *minutes* **Example:** `switch(config)# ldap-server deadtime 5`	Configures the global dead-time interval. The default value is 0 minutes. The range is from 1 to 60 minutes.

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

Step 4	(Optional) **show ldap-server** **Example:** `switch# show ldap-server`	Displays the LDAP server configuration.

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

Related Topics

Enabling LDAP, on page 143

Configuring AAA Authorization on LDAP Servers

You can configure the default AAA authorization method for LDAP servers.

Before you begin

Enable LDAP.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authorization** {**ssh-certificate** | **ssh-publickey**} **default** {**group** *group-list* | **local**}
3. **exit**
4. (Optional) **show aaa authorization** [**all**]
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**aaa authorization** {**ssh-certificate** | **ssh-publickey**} **default** {**group** *group-list* | **local**}
	Example:
	`switch(config)# aaa authorization ssh-certificate`
	`default group LDAPServer1 LDAPServer2`
		Configures the default AAA authorization method for the LDAP servers.
		The **ssh-certificate** keyword configures LDAP or local authorization with certificate authentication, and the **ssh-publickey** keyword configures LDAP or local authorization with the SSH public key. The default authorization is local authorization, which is the list of authorized commands for the user's assigned role.
		The *group-list* argument consists of a space-delimited list of LDAP server group names. Servers that belong to this group are contacted for AAA authorization. The **local** method uses the local database for authorization.

	Command or Action	Purpose

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

Step 4	(Optional) **show aaa authorization** [**all**] **Example:** `switch(config)# show aaa authorization`	Displays the AAA authorization configuration. The **all** keyword displays the default values.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling LDAP, on page 143

Disabling LDAP

You can disable LDAP.

Caution When you disable LDAP, all related configurations are automatically discarded.

SUMMARY STEPS

1. **configure terminal**
2. **no feature ldap**
3. **exit**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no feature ldap** **Example:** `switch(config)# no feature ldap`	Disables LDAP.

	Command or Action	Purpose

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

Step 4	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Monitoring LDAP Servers

You can monitor the statistics that the Cisco NX-OS device maintains for LDAP server activity.

Before you begin

Configure LDAP servers on the Cisco NX-OS device.

SUMMARY STEPS

1. **show ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} **Example:** `switch# show ldap-server statistics 10.10.1.1`	Displays the LDAP statistics.

Related Topics

Configuring LDAP Server Hosts, on page 144
Clearing LDAP Server Statistics, on page 158

Clearing LDAP Server Statistics

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

Before you begin

Configure LDAP servers on the Cisco NX-OS device.

SUMMARY STEPS

1. (Optional) **show ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

2. **clear ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **show ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} **Example:** `switch# show ldap-server statistics 10.10.1.1`	Displays the LDAP server statistics on the Cisco NX-OS device.
Step 2	**clear ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} **Example:** `switch# clear ldap-server statistics 10.10.1.1`	Clears the LDAP server statistics.

Related Topics

Configuring LDAP Server Hosts, on page 144
Monitoring LDAP Servers, on page 158

Verifying the LDAP Configuration

To display LDAP configuration information, perform one of the following tasks:

Command	Purpose
show running-config ldap [**all**]	Displays the LDAP configuration in the running configuration.
show startup-config ldap	Displays the LDAP configuration in the startup configuration.
show ldap-server	Displays LDAP configuration information.
show ldap-server groups	Displays LDAP server group configuration information.
show ldap-server statistics {*host-name* | *ipv4-address* | *ipv6-address*}	Displays LDAP statistics.
show ldap-search-map	Displays information about the configured LDAP attribute maps.

For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuration Examples for LDAP

The following example shows how to configure an LDAP server host and server group:

```
feature ldap
ldap-server host 10.10.2.2 enable-ssl
aaa group server ldap LdapServer
    server 10.10.2.2
exit
show ldap-server
show ldap-server groups
```

The following example shows how to configure an LDAP search map:

```
ldap search-map s0
userprofile attribute-name description search-filter
(&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
exit
show ldap-search-map
```

The following example shows how to configure AAA authorization with certificate authentication for an LDAP server:

```
aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2
exit
show aaa authorization
```

Where to Go Next

You can now configure AAA authentication methods to include the server groups.

Additional References for LDAP

This section includes additional information related to implementing LDAP.

Related Documents

Related Topic	Document Title
Cisco NX-OS licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
VRF configuration	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
• CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for LDAP

This table lists the release history for this feature.

Table 15: Feature History for LDAP

Feature Name	Releases	Feature Information
LDAP	6.0(1)	No change from Release 5.2.
LDAP	5.2(1)	The **ldap-server port** command was deprecated.
LDAP	5.1(1)	No change from Release 5.0.
LDAP	5.0(2)	This feature was introduced.

CHAPTER 8

Configuring SSH and Telnet

This chapter describes how to configure Secure Shell Protocol (SSH) and Telnet on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About SSH and Telnet

This section includes information about SSH and Telnet.

SSH Server

You can use the 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 user authentication mechanisms supported for SSH are RADIUS, TACACS+, LDAP, and the use of locally stored usernames and passwords.

SSH Client

The SSH client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco NX-OS device to make a secure, encrypted connection to another Cisco NX-OS device or to any other device that runs the 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 NX-OS software works with publicly and commercially available SSH servers.

SSH Server Keys

SSH requires server keys for secure communications to the Cisco NX-OS device. You can use SSH server 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 Algrorithm (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 two 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 NX-OS software generates an RSA key using 1024 bits.

SSH supports the following public key formats:

- OpenSSH
- IETF Secure Shell (SECSH)
- Public Key Certificate in Privacy-Enhanced Mail (PEM)

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

SSH Authentication Using Digital Certificates

SSH authentication on Cisco NX-OS devices provide X.509 digital certificate support for host authentication. An X.509 digital certificate is a data item that ensures the origin and integrity of a message. It contains encryption keys for secured communications and is signed by a trusted certification authority (CA) to verify the identity of the presenter. The X.509 digital certificate support provides either DSA or RSA algorithms for authentication.

The certificate infrastructure uses the first certificate that supports the Secure Socket Layer (SSL) and is returned by the security infrastructure, either through a query or a notification. Verification of certificates is successful if the certificates are from any of the trusted CAs configured and if not revoked or expired.

You can configure your device for either SSH authentication using an X.509 certificate or SSH authentication using a Public Key Certificate, but not both. If either of them is configured and the authentication fails, you are prompted for a password

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 device to the other. Telnet can accept either an IP address or a domain name as the remote device address.

The Telnet server is disabled by default on the Cisco NX-OS device.

Virtualization Support for SSH and Telnet

SSH and Telnet configuration and operation are local to the virtual device context (VDC). For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Prerequisites for SSH and Telnet

SSH and Telnet have the following prerequisites:

- You have configured IP on a Layer 3 interface, out-of-band on the mgmt 0 interface, or inband on an Ethernet interface.

Guidelines and Limitations for SSH and Telnet

SSH and Telnet have the following configuration guidelines and limitations:

- The Cisco NX-OS software supports only SSH version 2 (SSHv2).
- You can configure your device for either SSH authentication using an X.509 certificate or SSH authentication using a public key certificate but not both. If either of them is configured and the authentication fails, you are prompted for a password.
- Beginning in Cisco NX-OS Release 5.1, SSH runs in FIPS mode.
- The SFTP server feature does not support the regular SFTP **chown** and **chgrp** commands.
- When the SFTP server is enabled, only the admin user can use SFTP to access the switch.
- 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 Nexus device is reloaded unless a local user account with the same name as the remote user account is configured on the device before the SSH keys are imported.

Note 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.

Related Topics

Configuring FIPS, on page 17

Default Settings for SSH and Telnet

This table lists the default settings for SSH and Telnet parameters.

Table 16: Default SSH and Telnet Parameters

Parameters	Default
SSH server	Enabled
SSH server key	RSA key generated with 1024 bits
RSA key bits for generation	1024
Telnet server	Disabled
Telnet port number	23
Maximum number of SSH login attempts	3
SCP server	Disabled
SFTP server	Disabled

Configuring SSH

This section describes how to configure SSH.

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.

SUMMARY STEPS

1. **configure terminal**
2. **no feature ssh**
3. **ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]}
4. **feature ssh**
5. **exit**

6. (Optional) **show ssh key**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no feature ssh** **Example:** `switch(config)# no feature ssh`	Disables SSH.
Step 3	**ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]} **Example:** `switch(config)# ssh key rsa 2048`	Generates the SSH server key. The *bits* argument is the number of bits used to generate the RSA key. Beginning with Cisco NX-OS Release 5.1, the range is from 1024 to 2048. In Cisco NX-OS Release 5.0, The range is from 768 to 2048. The default value is 1024. You cannot specify the size of the DSA key. It is always set to 1024 bits. Use the **force** keyword to replace an existing key.
Step 4	**feature ssh** **Example:** `switch(config)# feature ssh`	Enables SSH.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 6	(Optional) **show ssh key** **Example:** `switch# show ssh key`	Displays the SSH server keys.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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 these formats:

- OpenSSH format
- IETF SECSH format
- Public Key Certificate in PEM format

Specifying the SSH Public Keys in IETF SECSH Format

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

Before you begin

Generate an SSH public key in IETF SCHSH format.

SUMMARY STEPS

1. **copy** *server-file* **bootflash:***filename*
2. **configure terminal**
3. **username** *username* **sshkey file bootflash:***filename*
4. **exit**
5. (Optional) **show user-account**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**copy** *server-file* **bootflash:***filename* **Example:** `switch# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub`	Downloads the file containing the SSH key in IETF SECSH format from a server. The server can be FTP, secure copy (SCP), secure FTP (SFTP), or TFTP.

Step 2	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 3	**username** *username* **sshkey file bootflash:***filename* **Example:** `switch(config)# username User1 sshkey file bootflash:secsh_file.pub`	Configures the SSH public key in IETF SECSH format.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 5	(Optional) **show user-account** **Example:** `switch# show user-account`	Displays the user account configuration.

	Command or Action	Purpose
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Specifying the SSH Public Keys in OpenSSH Format

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

Before you begin

Generate an SSH public key in OpenSSH format.

SUMMARY STEPS

1. **configure terminal**
2. **username** *username* **sshkey** *ssh-key*
3. **exit**
4. (Optional) **show user-account**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**username** *username* **sshkey** *ssh-key*
	Example:
	`switch(config)# username User1 sshkey`
	`ssh-rsa`
	`AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPj`
	`hOBYmsi6PAVKui1nIf/DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+`
	`XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5S4Tplx8=`
		Configures the SSH public key in OpenSSH format.

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

Step 4	(Optional) **show user-account** **Example:** `switch# show user-account`	Displays the user account configuration.

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

Configuring a Maximum Number of SSH Login Attempts

You can configure the maximum number of SSH login attempts. If the user exceeds the maximum number of permitted attempts, the session disconnects.

Note The total number of login attempts includes attempts through public-key authentication, certificate-based authentication, and password-based authentication. If public-key authentication is enabled, it takes priority. If only certificate-based and password-based authentication are enabled, certificate-based authentication takes priority. If you exceed the configured number of login attempts through all of these methods, a message appears indicating that too many authentication failures have occurred.

SUMMARY STEPS

1. **configure terminal**
2. **ssh login-attempts** *number*
3. (Optional) **show running-config security all**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ssh login-attempts** *number* **Example:** `switch(config)# ssh login-attempts 5`	Configures the maximum number of times that a user can attempt to log into an SSH session. The default maximum number of login attempts is 3. The range is from 1 to 10. **Note** The **no** form of this command removes the previous login attempts value and sets the maximum number of login attempts to the default value of 3.
Step 3	(Optional) **show running-config security all** **Example:** `switch(config)# show running-config security all`	Displays the configured maximum number of SSH login attempts.

	Command or Action	Purpose
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring a Login Grace Time for SSH Connections

You can configure the login grace time for SSH connections from remote devices to your Cisco NX-OS device. This configures the grace time for clients to authenticate themselves. If the time to login to the SSH session exceeds the specified grace time, the session disconnects and you will need to attempt logging in again.

Note Enable the SSH server on the remote device.

SUMMARY STEPS

1. **configure terminal**
2. **feature ssh**
3. **ssh login-gracetime** *number*
4. (Optional) **exit**
5. (Optional) **show running-config security**
6. (Optional) **show running-config security all**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**feature ssh**
	Example:
	`switch# feature ssh`
	`switch(config)#`
		Enables SSH.

Step 3	**ssh login-gracetime** *number* **Example:** `switch(config)# ssh login-gracetime 120`	Configures the login grace time in seconds for SSH connections from remote devices to your Cisco NX-OS device. The default login grace time is 120 seconds. The range is from 1 to 2147483647. **Note** The **no** form of this command removes the configured login grace time and resets it to the default value of 120 seconds.

	Command or Action	Purpose
Step 4	(Optional) **exit** **Example:** `switch(config)# exit`	Exits global configuration mode.
Step 5	(Optional) **show running-config security** **Example:** `switch(config)# show running-config security`	Displays the configured SSH login grace time.
Step 6	(Optional) **show running-config security all** **Example:** `switch(config)# show running-config security all`	Displays the configured or default SSH login grace time.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Starting SSH Sessions

You can start SSH sessions using IPv4 or IPv6 to connect to remote devices from the Cisco NX-OS device.

Before you begin

Obtain the hostname for the remote device and, if needed, the username on the remote device.

Enable the SSH server on the remote device.

SUMMARY STEPS

1. **ssh** [*username@*]{*ipv4-address* | *hostname*} [**vrf** *vrf-name*]
2. **ssh6** [*username@*]{*ipv6-address* | *hostname*} [**vrf** *vrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ssh** [*username@*]{*ipv4-address* | *hostname*} [**vrf** *vrf-name*] **Example:** `switch# ssh 10.10.1.1`	Creates an SSH IPv4 session to a remote device using IPv4. The default VRF is the default VRF.
Step 2	**ssh6** [*username@*]{*ipv6-address* | *hostname*} [**vrf** *vrf-name*] **Example:** `switch# ssh6 HostA`	Creates an SSH IPv6 session to a remote device using IPv6.

Starting SSH Sessions from Boot Mode

You can start SSH sessions from the boot mode of the Cisco NX-OS device to connect to remote devices.

Before you begin

Obtain the hostname for the remote device and, if needed, the username on the remote device.

Enable the SSH server on the remote device.

Ensure that the Cisco NX-OS device is loaded with only the kickstart image.

SUMMARY STEPS

1. **ssh** [*username***@**]*hostname*
2. **exit**
3. **copy scp:**//[*username***@**]*hostname*/*filepath directory*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ssh** [*username***@**]*hostname* **Example:** `switch(boot)# ssh user1@10.10.1.1`	Creates an SSH session to a remote device from the boot mode of the Cisco NX-OS device. The default VRF is always used.
Step 2	**exit** **Example:** `switch(boot)# exit`	Exits boot mode.
Step 3	**copy scp:**//[*username***@**]*hostname*/*filepath directory* **Example:** `switch# copy scp://user1@10.10.1.1/users abc`	Copies a file from the Cisco NX-OS device to a remote device using the Secure Copy Protocol (SCP). The default VRF is always used.

Configuring SSH Passwordless File Copy

You can copy files from a Cisco NX-OS device to a secure copy (SCP) or secure FTP (SFTP) server without a password. To do so, you must create an RSA or DSA identity that consists of public and private keys for authentication with SSH.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **username** *username* **keypair generate** {**rsa** [*bits* [**force**]] | **dsa** [**force**]}
3. (Optional) **show username** *username* **keypair**
4. **username** *username* **keypair export** {**bootflash:***filename* | **volatile:***filename*} {**rsa** | **dsa**} [**force**]
5. **username** *username* **keypair import** {**bootflash:***filename* | **volatile:***filename*} {**rsa** | **dsa**} [**force**]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **username** *username* **keypair generate** {**rsa** [*bits* [**force**]] | **dsa** [**force**]} **Example:** `switch(config)# username user1 keypair generate rsa 2048 force`	Generates the SSH public and private keys and stores them in the home directory ($HOME/.ssh) of the Cisco NX-OS device for the specified user. The Cisco NX-OS device uses the keys to communicate with the SSH server on the remote machine. The *bits* argument is the number of bits used to generate the key. Beginning with Cisco NX-OS Release 5.1, the range is from 1024 to 2048. In Cisco NX-OS Release 5.0, the range is from 768 to 2048. The default value is 1024. Use the **force** keyword to replace an existing key. The SSH keys are not generated if the **force** keyword is omitted and SSH keys are already present.
Step 3	(Optional) **show username** *username* **keypair** **Example:** `switch(config)# show username user1 keypair`	Displays the public key for the specified user. **Note** For security reasons, this command does not show the private key.
Step 4	Required: **username** *username* **keypair export** {**bootflash:***filename* | **volatile:***filename*} {**rsa** | **dsa**} [**force**] **Example:** `switch(config)# username user1 keypair export bootflash:key_rsa rsa`	Exports the public and private keys from the home directory of the Cisco NX-OS device to the specified bootflash or volatile directory. Use the **force** keyword to replace an existing key. The SSH keys are not exported if the **force** keyword is omitted and SSH keys are already present. To export the generated key pair, you are prompted to enter a passphrase that encrypts the private key. The private key is exported as the file that you specify, and the public key is exported with the same filename followed by a .pub extension. You can now copy this key pair to any Cisco NX-OS device and use SCP or SFTP to copy the public key file (*.pub) to the home directory of the server. **Note** For security reasons, this command can be executed only from global configuration mode.
Step 5	Required: **username** *username* **keypair import** {**bootflash:***filename* | **volatile:***filename*} {**rsa** | **dsa**} [**force**] **Example:** `switch(config)# username user1 keypair import bootflash:key_rsa rsa`	Imports the exported public and private keys from the specified bootflash or volatile directory to the home directory of the Cisco NX-OS device. Use the **force** keyword to replace an existing key. The SSH keys are not imported if the **force** keyword is omitted and SSH keys are already present.

	Command or Action	Purpose
		To import the generated key pair, you are prompted to enter a passphrase that decrypts the private key. The private key is imported as the file that you specify, and the public key is imported with the same filename followed by a .pub extension. **Note** For security reasons, this command can be executed only from global configuration mode. **Note** Only the users whose keys are configured on the server are able to access the server without a password.

What to do next

On the SCP or SFTP server, use the following command to append the public key stored in the *.pub file (for example, key_rsa.pub) to the authorized_keys file:

$ cat key_rsa.pub >> $HOME/.ssh/ authorized_keys

You can now copy files from the Cisco NX-OS device to the server without a password using standard SSH and SCP commands.

Configuring SCP and SFTP Servers

You can configure an SCP or SFTP server on the Cisco NX-OS device in order to copy files to and from a remote device. After you enable the SCP or SFTP server, you can execute an SCP or SFTP command on the remote device to copy the files to or from the Cisco NX-OS device.

Note The arcfour and blowfish cipher options are not supported for the SCP server.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **feature scp-server**
3. [**no**] **feature sftp-server**
4. **exit**
5. (Optional) **show running-config security**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
Step 2	[**no**] **feature scp-server** **Example:** `switch(config)# feature scp-server`	Enables or disables the SCP server on the Cisco NX-OS device.
Step 3	Required: [**no**] **feature sftp-server** **Example:** `switch(config)# feature sftp-server`	Enables or disables the SFTP server on the Cisco NX-OS device.

Step 4	Required: **exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 5	(Optional) **show running-config security** **Example:** `switch# show running-config security`	Displays the configuration status of the SCP and SFTP servers.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Clearing SSH Hosts

When you download a file from a server using SCP or SFTP, or when you start an SSH session from this device to a remote host, you establish a trusted SSH relationship with that server. You can clear the list of trusted SSH servers for your user account.

SUMMARY STEPS

1. **clear ssh hosts**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clear ssh hosts** **Example:** `switch# clear ssh hosts`	Clears the SSH host sessions and the known host file.

Disabling the SSH Server

By default, the SSH server is enabled on the Cisco NX-OS device. You can disable the SSH server to prevent SSH access to the switch.

SUMMARY STEPS

1. **configure terminal**
2. **no feature ssh**
3. **exit**
4. (Optional) **show ssh server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no feature ssh** **Example:** `switch(config)# no feature ssh`	Disables SSH.

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

Step 4	(Optional) **show ssh server** **Example:** `switch# show ssh server`	Displays the SSH server configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Deleting SSH Server Keys

You can delete SSH server keys on the Cisco NX-OS device after you disable the SSH server.

Note To reenable SSH, you must first generate an SSH server key.

SUMMARY STEPS

1. **configure terminal**
2. **no feature ssh**
3. **no ssh key** [**dsa** | **rsa**]
4. **exit**

5. (Optional) **show ssh key**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no feature ssh** **Example:** `switch(config)# no feature ssh`	Disables SSH.
Step 3	**no ssh key** [**dsa** | **rsa**] **Example:** `switch(config)# no ssh key rsa`	Deletes the SSH server key. The default is to delete all the SSH keys.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 5	(Optional) **show ssh key** **Example:** `switch# show ssh key`	Displays the SSH server key configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Generating SSH Server Keys, on page 166

Clearing SSH Sessions

You can clear SSH sessions from the Cisco NX-OS device.

SUMMARY STEPS

1. **show users**
2. **clear line** *vty-line*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show users** **Example:** `switch# show users`	Displays user session information.
Step 2	**clear line** *vty-line* **Example:** `switch(config)# clear line pts/12`	Clears a user SSH session.

Configuring Telnet

This section describes how to configure Telnet on the Cisco NX-OS device.

Enabling the Telnet Server

You can enable the Telnet server on the Cisco NX-OS device. By default, the Telnet server is disabled.

SUMMARY STEPS

1. **configure terminal**
2. **feature telnet**
3. **exit**
4. (Optional) **show telnet server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**feature telnet** **Example:** `switch(config)# feature telnet`	Enables the Telnet server. The default is disabled.

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

	Command or Action	Purpose
Step 4	(Optional) **show telnet server** **Example:** `switch# show telnet server`	Displays the Telnet server configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Starting Telnet Sessions to Remote Devices

You can start Telnet sessions to connect to remote devices from the Cisco NX-OS device. You can start Telnet sessions using either IPv4 or IPv6.

Before you begin

Obtain the hostname or IP address for the remote device and, if needed, the username on the remote device.

Enable the Telnet server on the Cisco NX-OS device.

Enable the Telnet server on the remote device.

SUMMARY STEPS

1. **telnet** {*ipv4-address* | *host-name*} [*port-number*] [**vrf** *vrf-name*]
2. **telnet6** {*ipv6-address* | *host-name*} [*port-number*] [**vrf** *vrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**telnet** {*ipv4-address* | *host-name*} [*port-number*] [**vrf** *vrf-name*] **Example:** `switch# telnet 10.10.1.1`	Starts a Telnet session to a remote device using IPv4. The default port number is 23. The range is from 1 to 65535. The default VRF is the default VRF.
Step 2	**telnet6** {*ipv6-address* | *host-name*} [*port-number*] [**vrf** *vrf-name*] **Example:** `switch# telnet6 2001:0DB8::ABCD:1 vrf management`	Starts a Telnet session to a remote device using IPv6. The default port number is 23. The range is from 1 to 65535. The default VRF is the default VRF.

Related Topics

Enabling the Telnet Server, on page 179

Clearing Telnet Sessions

You can clear Telnet sessions from the Cisco NX-OS device.

Before you begin

Enable the Telnet server on the Cisco NX-OS device.

SUMMARY STEPS

1. **show users**
2. **clear line** *vty-line*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show users** **Example:** `switch# show users`	Displays user session information.
Step 2	**clear line** *vty-line* **Example:** `switch(config)# clear line pts/12`	Clears a user Telnet session.

Verifying the SSH and Telnet Configuration

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

Command	Purpose
show ssh key [**dsa** | **rsa**]	Displays SSH server key-pair information.
show running-config security [**all**]	Displays the SSH and user account configuration in the running configuration. The **all** keyword displays the default values for the SSH and user accounts.
show ssh server	Displays the SSH server configuration.
show telnet server	Displays the Telnet server configuration.
show username *username* **keypair**	Displays the public key for the specified user.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuration Example for SSH

The following example shows how to configure SSH with an OpenSSH key:

Step 1 Disable the SSH server.

Example:

```
switch# configure terminal
switch(config)# no feature ssh
```

Step 2 Generate an SSH server key.

Example:

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

Step 3 Enable the SSH server.

Example:

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

Step 4 Display the SSH server key.

Example:

```
switch(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2007

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr
+MZm99n2U0ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K36lr39
HmXL6VgpRVn1XQFiBwn4na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhFhoNE=

bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
**************************************
could not retrieve dsa key information
**************************************
```

Step 5 Specify the SSH public key in OpenSSH format.

Example:

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50r
v7gsEPjhOBYmsi6PAVKui1nIf/DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQ
W3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5
4Tplx8=
```

Step 6 Save the configuration.

Example:

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

Configuration Example for SSH Passwordless File Copy

The following example shows how to copy files from a Cisco NX-OS device to a secure copy (SCP) or secure FTP (SFTP) server without a password:

Step 1 Generate the SSH public and private keys and store them in the home directory of the Cisco NX-OS device for the specified user.

Example:

```
switch# configure terminal
switch(config)# username admin keypair generate rsa
generating rsa key(1024 bits)......
generated rsa key
```

Step 2 Display the public key for the specified user.

Example:

```
switch(config)# show username admin keypair

**************************************

rsa Keys generated: Thu Jul  9 11:10:29 2009

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZElTfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
**************************************

could not retrieve dsa key information
**************************************
```

Step 3 Export the public and private keys from the home directory of the Cisco NX-OS device to the specified bootflash directory.

Example:

```
switch(config)# username admin keypair export bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# dir
.
.
.
        951     Jul 09 11:13:59 2009  key_rsa
        221     Jul 09 11:14:00 2009  key_rsa.pub
.
.
```

Step 4 After copying these two files to another Cisco NX-OS device using the **copy scp** or **copy sftp** command, import them to the home directory of the Cisco NX-OS device.

Example:

```
switch(config)# username admin keypair import bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# show username admin keypair
**************************************

rsa Keys generated: Thu Jul  9 11:10:29 2009

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZElTfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
**************************************

could not retrieve dsa key information
**************************************
switch(config)#
```

Step 5 On the SCP or SFTP server, append the public key stored in key_rsa.pub to the authorized_keys file.

Example:

```
$ cat key_rsa.pub >> $HOME/.ssh/ authorized_keys
```

You can now copy files from the Cisco NX-OS device to the server without a password using standard SSH and SCP commands.

Step 6 (Optional) Repeat this procedure for the DSA keys.

Additional References for SSH and Telnet

This section describes additional information related to implementing SSH and Telent.

Related Documents

Related Topic	Document Title
Cisco NX-OS licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
VRF configuration	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

CHAPTER 9

Configuring PKI

This chapter describes the Public Key Infrastructure (PKI) support on the Cisco NX-OS device. PKI allows the device to obtain and use digital certificates for secure communication in the network and provides manageability and scalability for Secure Shell (SSH).

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About PKI

This section provides information about PKI.

CAs and Digital Certificates

Certificate authorities (CAs) manage certificate requests and issue certificates to participating entities such as hosts, network devices, or users. The CAs provide centralized key management for the participating entities.

Digital signatures, based on public key cryptography, digitally authenticate devices and individual users. In public key cryptography, such as the RSA encryption system, each device or user has a key pair that contains both a private key and a public key. The private key is kept secret and is known only to the owning device or user only. However, the public key is known to everybody. Anything encrypted with one of the keys can be decrypted with the other. A signature is formed when data is encrypted with a sender's private key. The receiver verifies the signature by decrypting the message with the sender's public key. This process relies on the receiver having a copy of the sender's public key and knowing with a high degree of certainty that it really does belong to the sender and not to someone pretending to be the sender.

Digital certificates link the digital signature to the sender. A digital certificate contains information to identify a user or device, such as the name, serial number, company, department, or IP address. It also contains a copy of the entity's public key. The CA that signs the certificate is a third party that the receiver explicitly trusts to validate identities and to create digital certificates.

To validate the signature of the CA, the receiver must first know the CA's public key. Typically, this process is handled out of band or through an operation done at installation. For instance, most web browsers are configured with the public keys of several CAs by default.

Trust Model, Trust Points, and Identity CAs

The PKI trust model is hierarchical with multiple configurable trusted CAs. You can configure each participating device with a list of trusted CAs so that a peer certificate obtained during the security protocol exchanges can be authenticated if it was issued by one of the locally trusted CAs. The Cisco NX-OS software locally stores the self-signed root certificate of the trusted CA (or certificate chain for a subordinate CA). The process of securely obtaining a trusted CA's root certificate (or the entire chain in the case of a subordinate CA) and storing it locally is called *CA authentication*.

The information about a trusted CA that you have configured is called the *trust point* and the CA itself is called a *trust point CA*. This information consists of a CA certificate (or certificate chain in case of a subordinate CA) and certificate revocation checking information.

The Cisco NX-OS device can also enroll with a trust point to obtain an identity certificate to associate with a key pair. This trust point is called an *identity CA*.

RSA Key Pairs and Identity Certificates

You can obtain an identity certificate by generating one or more RSA key pairs and associating each RSA key pair with a trust point CA where the Cisco NX-OS device intends to enroll. The Cisco NX-OS device needs only one identity per CA, which consists of one key pair and one identity certificate per CA.

The Cisco NX-OS software allows you to generate RSA key pairs with a configurable key size (or modulus). The default key size is 512. You can also configure an RSA key-pair label. The default key label is the device fully qualified domain name (FQDN).

The following list summarizes the relationship between trust points, RSA key pairs, and identity certificates:

- A trust point corresponds to a specific CA that the Cisco NX-OS device trusts for peer certificate verification for any application (such as SSH).
- A Cisco NX-OS device can have many trust points and all applications on the device can trust a peer certificate issued by any of the trust point CAs.
- A trust point is not restricted to a specific application.
- A Cisco NX-OS device enrolls with the CA that corresponds to the trust point to obtain an identity certificate. You can enroll your device with multiple trust points which means that you can obtain a separate identity certificate from each trust point. The identity certificates are used by applications

depending upon the purposes specified in the certificate by the issuing CA. The purpose of a certificate is stored in the certificate as a certificate extension.

- When enrolling with a trust point, you must specify an RSA key pair to be certified. This key pair must be generated and associated to the trust point before generating the enrollment request. The association between the trust point, key pair, and identity certificate is valid until it is explicitly removed by deleting the certificate, key pair, or trust point.
- The subject name in the identity certificate is the fully qualified domain name for the Cisco NX-OS device.
- You can generate one or more RSA key pairs on a device and each can be associated to one or more trust points. But no more than one key pair can be associated to a trust point, which means only one identity certificate is allowed from a CA.
- If the Cisco NX-OS device obtains multiple identity certificates (each from a distinct CA), the certificate that an application selects to use in a security protocol exchange with a peer is application specific.
- You do not need to designate one or more trust points for an application. Any application can use any certificate issued by any trust point as long as the certificate purpose satisfies the application requirements.
- You do not need more than one identity certificate from a trust point or more than one key pair to be associated to a trust point. A CA certifies a given identity (or name) only once and does not issue multiple certificates with the same name. If you need more than one identity certificate for a CA and if the CA allows multiple certificates with the same names, you must define another trust point for the same CA, associate another key pair to it, and have it certified.

Multiple Trusted CA Support

The Cisco NX-OS device can trust multiple CAs by configuring multiple trust points and associating each with a distinct CA. With multiple trusted CAs, you do not have to enroll a device with the specific CA that issued the certificate to a peer. Instead, you can configure the device with multiple trusted CAs that the peer trusts. The Cisco NX-OS device can then use a configured trusted CA to verify certificates received from a peer that were not issued by the same CA defined in the identity of the peer device.

PKI Enrollment Support

Enrollment is the process of obtaining an identity certificate for the device that is used for applications like SSH. It occurs between the device that requests the certificate and the certificate authority.

The Cisco NX-OS device performs the following steps when performing the PKI enrollment process:

- Generates an RSA private and public key pair on the device.
- Generates a certificate request in standard format and forwards it to the CA.

Note The CA administrator may be required to manually approve the enrollment request at the CA server, when the request is received by the CA.

- Receives the issued certificate back from the CA, signed with the CA's private key.

- Writes the certificate into a nonvolatile storage area on the device (bootflash).

Manual Enrollment Using Cut-and-Paste

The Cisco NX-OS software supports certificate retrieval and enrollment using manual cut-and-paste. Cut-and-paste enrollment means that you must cut and paste the certificate requests and resulting certificates between the device and the CA.

You must perform the following steps when using cut and paste in the manual enrollment process:

- Create an enrollment certificate request, which the Cisco NX-OS device displays in base64-encoded text form.
- Cut and paste the encoded certificate request text in an e-mail or in a web form and send it to the CA.
- Receive the issued certificate (in base64-encoded text form) from the CA in an e-mail or in a web browser download.
- Cut and paste the issued certificate to the device using the certificate import facility.

Multiple RSA Key Pair and Identity CA Support

Multiple identity CAs enable the device to enroll with more than one trust point, which results in multiple identity certificates, each from a distinct CA. With this feature, the Cisco NX-OS device can participate in SSH and other applications with many peers using certificates issued by CAs that are acceptable to those peers.

The multiple RSA key-pair feature allows the device to maintain a distinct key pair for each CA with which it is enrolled. It can match policy requirements for each CA without conflicting with the requirements specified by the other CAs, such as the key length. The device can generate multiple RSA key pairs and associate each key pair with a distinct trust point. Thereafter, when enrolling with a trust point, the associated key pair is used to construct the certificate request.

Peer Certificate Verification

The PKI support on a Cisco NX-OS device can verify peer certificates. The Cisco NX-OS software verifies certificates received from peers during security exchanges for applications, such as SSH. The applications verify the validity of the peer certificates. The Cisco NX-OS software performs the following steps when verifying peer certificates:

- Verifies that the peer certificate is issued by one of the locally trusted CAs.
- Verifies that the peer certificate is valid (not expired) with respect to current time.
- Verifies that the peer certificate is not yet revoked by the issuing CA.

For revocation checking, the Cisco NX-OS software supports the certificate revocation list (CRL). A trust point CA can use this method to verify that the peer certificate has not been revoked.

Certificate Revocation Checking

The Cisco NX-OS software can check the revocation status of CA certificates. The applications can use the revocation checking mechanisms in the order that you specify. The choices are CRL, none, or a combination of these methods.

CRL Support

The CAs maintain certificate revocation lists (CRLs) to provide information about certificates revoked prior to their expiration dates. The CAs publish the CRLs in a repository and provide the download public URL in all issued certificates. A client verifying a peer's certificate can obtain the latest CRL from the issuing CA and use it to determine if the certificate has been revoked. A client can cache the CRLs of some or all of its trusted CAs locally and use them later if necessary until the CRLs expire.

The Cisco NX-OS software allows the manual configuration of predownloaded CRLs for the trust points, and then caches them in the device bootflash (cert-store). During the verification of a peer certificate, the Cisco NX-OS software checks the CRL from the issuing CA only if the CRL has already been cached locally and the revocation checking is configured to use the CRL. Otherwise, the Cisco NX-OS software does not perform CRL checking and considers the certificate to be not revoked unless you have configured other revocation checking methods.

Import and Export Support for Certificates and Associated Key Pairs

As part of the CA authentication and enrollment process, the subordinate CA certificate (or certificate chain) and identity certificates can be imported in standard PEM (base64) format.

The complete identity information in a trust point can be exported to a file in the password-protected PKCS#12 standard format. It can be later imported to the same device (for example, after a system crash) or to a replacement device. The information in a PKCS#12 file consists of the RSA key pair, the identity certificate, and the CA certificate (or chain).

Virtualization Support for PKI

The configuration and operation of the PKI feature is local to the virtual device context (VDC). For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Guidelines and Limitations for PKI

PKI has the following configuration guidelines and limitations:

- The maximum number of key pairs you can configure on a Cisco NX-OS device is 16.
- The maximum number of trust points you can declare on a Cisco NX-OS device is 16.
- The maximum number of identify certificates you can configure on a Cisco NX-OS device is 16.
- The maximum number of certificates in a CA certificate chain is 10.
- The maximum number of trust points you can authenticate to a specific CA is 10.
- Configuration rollbacks do not support the PKI configuration.

- The Cisco NX-OS software does not support OSCP.

Note 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 PKI

This table lists the default settings for PKI parameters.

Table 17: Default PKI Parameters

Parameters	Default
Trust point	None
RSA key pair	None
RSA key-pair label	Device FQDN
RSA key-pair modulus	512
RSA key-pair exportable	Enabled
Revocation check method	CRL
Cert-store for certificate authentication	local

Configuring CAs and Digital Certificates

This section describes the tasks that you must perform to allow CAs and digital certificates on your Cisco NX-OS device to interoperate.

Configuring the Hostname and IP Domain Name

You must configure the hostname and IP domain name of the device if you have not yet configured them because the Cisco NX-OS software uses the fully qualified domain name (FQDN) of the device as the subject in the identity certificate. Also, the Cisco NX-OS software uses the device FQDN as a default key label when you do not specify a label during key-pair generation. For example, a certificate named DeviceA.example.com is based on a device hostname of DeviceA and a device IP domain name of example.com.

Caution Changing the hostname or IP domain name after generating the certificate can invalidate the certificate.

SUMMARY STEPS

1. **configure terminal**
2. **hostname** *hostname*
3. **ip domain-name** *name* [**use-vrf** *vrf-name*]
4. **exit**
5. (Optional) **show hosts**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**hostname** *hostname* **Example:** `switch(config)# hostname DeviceA`	Configures the hostname of the device.
Step 3	**ip domain-name** *name* [**use-vrf** *vrf-name*] **Example:** `DeviceA(config)# ip domain-name example.com`	Configures the IP domain name of the device. If you do not specify a VRF name, the command uses the default VRF.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show hosts** **Example:** `switch# show hosts`	Displays the IP domain name.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Generating an RSA Key Pair

You can generate an RSA key pairs to sign and/or encrypt and decrypt the security payload during security protocol exchanges for applications. You must generate the RSA key pair before you can obtain a certificate for your device.

SUMMARY STEPS

1. **configure terminal**

2. **crypto key generate rsa** [**label** *label-string*] [**exportable**] [**modulus** *size*]
3. **exit**
4. (Optional) **show crypto key mypubkey rsa**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**crypto key generate rsa** [**label** *label-string*] [**exportable**] [**modulus** *size*] **Example:** `switch(config)# crypto key generate rsa exportable`	Generates an RSA key pair. The maximum number of key pairs on a device is 16. The label string is alphanumeric, case sensitive, and has a maximum length of 64 characters. The default label string is the hostname and the FQDN separated by a period character (.). Valid modulus values are 512, 768, 1024, 1536, and 2048. The default modulus size is 512. **Note** The security policy on the Cisco NX-OS device and on the CA (where enrollment is planned) should be considered when deciding the appropriate key modulus. By default, the key pair is not exportable. Only exportable key pairs can be exported in the PKCS#12 format. **Caution** You cannot change the exportability of a key pair.

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

Step 4	(Optional) **show crypto key mypubkey rsa** **Example:** `switch# show crypto key mypubkey rsa`	Displays the generated key.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Creating a Trust Point CA Association

You must associate the Cisco NX-OS device with a trust point CA.

Before you begin

Generate the RSA key pair.

SUMMARY STEPS

1. **configure terminal**
2. **crypto ca trustpoint** *name*
3. **enrollment terminal**
4. **rsakeypair** *label*
5. **exit**
6. (Optional) **show crypto ca trustpoints**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**crypto ca trustpoint** *name*
	Example:
	`switch(config)# crypto ca trustpoint admin-ca`
	`switch(config-trustpoint)#`
		Declares a trust point CA that the device should trust and enters trust point configuration mode.
		Note The maximum number of trust points that you can configure on a device is 16.

Step 3	**enrollment terminal** **Example:** `switch(config-trustpoint)# enrollment terminal`	Enables manual cut-and-paste certificate enrollment. The default is enabled. **Note** The Cisco NX-OS software supports only the manual cut-and-paste method for certificate enrollment.
Step 4	**rsakeypair** *label* **Example:** `switch(config-trustpoint)# rsakeypair SwitchA`	Specifies the label of the RSA key pair to associate to this trust point for enrollment. **Note** You can specify only one RSA key pair per CA.

Step 5	**exit**
	Example:
	`switch(config-trustpoint)# exit`
	`switch(config)#`
		Exits trust point configuration mode.

	Command or Action	Purpose
Step 6	(Optional) **show crypto ca trustpoints** **Example:** `switch(config)# show crypto ca trustpoints`	Displays trust point information.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Generating an RSA Key Pair, on page 193

Configuring the Cert-Store for Certificate Authentication

You can specify the cert-store for certificate authentication. By default, the application certificate is authenticated against the CA certificate that is available from the local cert-store (the Cisco NX-OS device). If your application requires the CA certificate to reside remotely, you can configure a Lightweight Directory Access Protocol (LDAP) server as a remote cert-store.

Before you begin

If you plan to configure a remote cert-store, set up an LDAP server in a remote device and make sure that the CA certificates that are used for authentication are loaded to the Active Directory.

SUMMARY STEPS

1. **configure terminal**
2. **crypto ca lookup** {**local** | **remote** | **both**}
3. (Optional) **show crypto ca certstore**
4. (Optional) **crypto ca remote ldap server-group** *group-name*
5. (Optional) **crypto ca remote ldap crl-refresh-time** *hours*
6. (Optional) **show crypto ca remote-certstore**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**crypto ca lookup** {**local** | **remote** | **both**} **Example:** `switch(config)# crypto ca lookup remote`	Authenticates the application certificate against the CA certificate that is available in the local or remote cert-store. The default is local. If you choose both, the application certificate is authenticated against the local cert-store, but

	Command or Action	Purpose
		if the authentication fails or the CA certificate is not found, the remote cert-store is used. **Note** The **crypto ca lookup** commands are not add-on commands. Each command overwrites the existing one.
Step 3	(Optional) **show crypto ca certstore** **Example:** `switch(config)# show crypto ca certstore`	Displays the cert-store configuration.
Step 4	(Optional) **crypto ca remote ldap server-group** *group-name* **Example:** `switch(config)# crypto ca remote ldap server-group group1`	If you configured a remote cert-store, configures the LDAP server group to be used while communicating with LDAP. You can enter up to 64 alphanumeric characters for the server group name.
Step 5	(Optional) **crypto ca remote ldap crl-refresh-time** *hours* **Example:** `switch(config)# crypto ca remote ldap crl-refresh-time 10`	If you configured a remote cert-store and the LDAP server group, configures the refresh time to update the certificate revocation list (CRL) from the remote cert-store. The CRL is a list of CA certificates that have been revoked and are no longer valid. The refresh time ranges from 0 to 744 hours. If you enter 0, the refresh routine runs once.
Step 6	(Optional) **show crypto ca remote-certstore** **Example:** `switch(config)# show crypto ca remote-certstore`	Displays the remote cert-store configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring Certificate Mapping Filters, on page 197

Configuring Certificate Mapping Filters

You can configure mapping filters to validate the CA certificates that are used for authentication. The mapping filters are used to match the CA certificate against a username.

Cisco NX-OS supports the following certificate mapping filters:

- %username%—Substitutes the user's login name.
- %username-without-domain%—Substitutes the user's login name without the domain (in Windows only).
- %hostname%—Substitutes the peer hostname.

- *—Supports a wild character.

Before you begin

Configure a cert-store for certificate authentication.

SUMMARY STEPS

1. **configure terminal**
2. **crypto certificatemap mapname** *map-name*
3. **filter** [**subject-name** *subject-name* | **altname-email** *e-mail-ID* | **altname-upn** *user-principal-name*]
4. **exit**
5. (Optional) **crypto cert ssh-authorize** [**default** | *issuer-CAname*] [**map** *map-name1* [*map-name2*]]
6. (Optional) **show crypto certificatemap**
7. (Optional) **show crypto ssh-auth-map**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**crypto certificatemap mapname** *map-name* **Example:** `switch(config)# crypto certificatemap mapname filtermap1`	Creates a new filter map.

Step 3	**filter** [**subject-name** *subject-name* | **altname-email** *e-mail-ID* | **altname-upn** *user-principal-name*]
	Example:
	`switch(config-certmap-filter)# filter altname-email jsmith@acme.com`
		Configures one or more certificate mapping filters within the filter map. These certificate field attributes are supported in the filters:
		• subject-name—The required subject name in the LDAP distinguished name (DN) string format. For example:
		`filter subject-name cn=%username%,ou=PKI,o=Acme,c=US`
		• altname-email—The e-mail address that must be present in the certificate as a subject alternative name. For example:
		`filter altname-email %username%@*`
		• altname-upn—The principal name that must be present in the certificate as a subject alternative name. For example:
		`filter altname-upn %username-without-domain%@%hostname%`

	Command or Action	Purpose
		The validation passes if the certificate passes all of the filters configured in the map.

Step 4	**exit**
	Example:
	`switch(config-certmap-filter)# exit`
	`switch(config)#`
		Exits certificate mapping filter configuration mode.

Step 5	(Optional) **crypto cert ssh-authorize** [**default** | *issuer-CAname*] [**map** *map-name1* [*map-name2*]] **Example:** `switch(config)# crypto cert ssh-authorize default map filtermap1`	Configures a certificate mapping filter for the Secure Shell (SSH) protocol. You can use the default filter map for SSH authorization or specify the issuer of the CA certificate. If you do not use the default map, you can specify one or two filter maps for authorization. If you specify the issuer of the CA certificate, the certificate bound to the user account is validated as successful if it passes one of the configured maps.
Step 6	(Optional) **show crypto certificatemap** **Example:** `switch(config)# show crypto certificatemap`	Displays the certificate mapping filters.
Step 7	(Optional) **show crypto ssh-auth-map** **Example:** `switch(config)# show crypto ssh-auth-map`	Displays the mapping filters configured for SSH authentication.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring the Cert-Store for Certificate Authentication, on page 196

Authenticating the CA

The configuration process of trusting a CA is complete only when the CA is authenticated to the Cisco NX-OS device. You must authenticate your Cisco NX-OS device to the CA by obtaining the self-signed certificate of the CA in PEM format, which contains the public key of the CA. Because the certificate of the CA is self-signed (the CA signs its own certificate) the public key of the CA should be manually authenticated by contacting the CA administrator to compare the fingerprint of the CA certificate.

Note The CA that you are authenticating is not a self-signed CA when it is a subordinate CA to another CA, which itself may be a subordinate to yet another CA, and so on, finally ending in a self-signed CA. This type of CA certificate is called the *CA certificate chain* of the CA being authenticated. In this case, you must input the full list of the CA certificates of all the CAs in the certification chain during the CA authentication. The maximum number of certificates in a CA certificate chain is 10.

Before you begin

Create an association with the CA.

Obtain the CA certificate or CA certificate chain.

SUMMARY STEPS

1. **configure terminal**
2. **crypto ca authenticate** *name*
3. **exit**
4. (Optional) **show crypto ca trustpoints**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**crypto ca authenticate** *name*
	Example:
	`switch(config)# crypto ca authenticate admin-ca`
	`input (cut & paste) CA certificate (chain) in PEM`
	` format;`
	`end the input with a line containing only END OF`
	`INPUT :`
	`-----BEGIN CERTIFICATE-----`
	`MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB`
	`kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO`
	`MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE`
	`ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD`
	`QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN`
	`AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth`
	`cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG`
	`A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN`
	`AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI`
	`OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E`
	`BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ`
	`GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs`
	`L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XEN1cnRFbnJv`
	`bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB`
	`BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea`
	`NBG7E0oN66zex0EOEfG1Vs6mXp1//w==`
	`-----END CERTIFICATE-----`
	`END OF INPUT`
	`Fingerprint(s): MD5`
	`Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12`
	`Do you accept this certificate? [yes/no]: yes`
		Prompts you to cut and paste the certificate of the CA. Use the same name that you used when declaring the CA.
		The maximum number of trust points that you can authenticate to a specific CA is 10.
		Note For subordinate CA authentication, the Cisco NX-OS software requires the full chain of CA certificates ending in a self-signed CA because the CA chain is needed for certificate verification as well as for PKCS#12 format export.

Step 3	**exit** **Example:**	Exits configuration mode.

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	
Step 4	(Optional) **show crypto ca trustpoints** **Example:** `switch# show crypto ca trustpoints`	Displays the trust point CA information.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Creating a Trust Point CA Association, on page 195

Configuring Certificate Revocation Checking Methods

During security exchanges with a client (for example, an SSH user), the Cisco NX-OS device performs the certificate verification of the peer certificate sent by the client. The verification process may involve certificate revocation status checking.

You can configure the device to check the CRL downloaded from the CA. Downloading the CRL and checking locally does not generate traffic in your network. However, certificates can be revoked between downloads and your device would not be aware of the revocation.

Before you begin

Authenticate the CA.

Ensure that you have configured the CRL if you want to use CRL checking.

SUMMARY STEPS

1. **configure terminal**
2. **crypto ca trustpoint** *name*
3. **revocation-check** {**crl** [**none**] | **none**}
4. **exit**
5. (Optional) **show crypto ca trustpoints**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**crypto ca trustpoint** *name*
	Example:
	`switch(config)# crypto ca trustpoint admin-ca`
	`switch(config-trustpoint)#`
		Specifies a trust point CA and enters trust point configuration mode.

Step 3	**revocation-check** {**crl** [**none**] | **none**} **Example:** `switch(config-trustpoint)# revocation-check none`	Configures the certificate revocation checking methods. The default method is **crl**. The Cisco NX-OS software uses the certificate revocation methods in the order that you specify.

Step 4	**exit**
	Example:
	`switch(config-trustpoint)# exit`
	`switch(config)#`
		Exits trust point configuration mode.

Step 5	(Optional) **show crypto ca trustpoints** **Example:** `switch(config)# show crypto ca trustpoints`	Displays the trust point CA information.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Authenticating the CA, on page 199
Configuring a CRL, on page 208

Generating Certificate Requests

You must generate a request to obtain identity certificates from the associated trust point CA for each of your device's RSA key pairs. You must then cut and paste the displayed request into an e-mail or in a website form for the CA.

Before you begin

Create an association with the CA.

Obtain the CA certificate or CA certificate chain.

SUMMARY STEPS

1. **configure terminal**
2. **crypto ca enroll** *name*
3. **exit**
4. (Optional) **show crypto ca certificates**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td>Step 1</td><td>configure terminal
Example:<pre>
switch# configure terminal
switch(config)#
</pre></td><td>Enters global configuration mode.</td></tr>
<tr><td>Step 2</td><td>crypto ca enroll name
Example:<pre>
switch(config)# crypto ca enroll admin-ca
Create the certificate request ..
 Create a challenge password. You will need to
verbally provide this
  password to the CA Administrator in order to
revoke your certificate.
  For security reasons your password will not be
saved in the configuration.
  Please make a note of it.
  Password:nbv123
 The subject name in the certificate will be:
DeviceA.cisco.com
 Include the switch serial number in the subject
name? [yes/no]: no
 Include an IP address in the subject name
[yes/no]: yes
ip address:172.22.31.162
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
</pre></td><td>Generates a certificate request for an authenticated CA.
Note You must remember the challenge password. It is not saved with the configuration. You must enter this password if your certificate needs to be revoked.</td></tr>
<tr><td>Step 3</td><td>exit
Example:<pre>
switch(config-trustpoint)# exit
switch(config)#
</pre></td><td>Exits trust point configuration mode.</td></tr>
<tr><td>Step 4</td><td>(Optional) show crypto ca certificates
Example:<pre>
switch(config)# show crypto ca certificates
</pre></td><td>Displays the CA certificates.</td></tr>
<tr><td>Step 5</td><td>(Optional) copy running-config startup-config
Example:<pre>
switch(config)# copy running-config startup-config
</pre></td><td>Copies the running configuration to the startup configuration.</td></tr>
</table>

Related Topics

Creating a Trust Point CA Association, on page 195

Installing Identity Certificates

You can receive the identity certificate from the CA by e-mail or through a web browser in base64 encoded text form. You must install the identity certificate from the CA by cutting and pasting the encoded text.

Before you begin

Create an association with the CA.

Obtain the CA certificate or CA certificate chain.

SUMMARY STEPS

1. **configure terminal**
2. **crypto ca import** *name* **certificate**
3. **exit**
4. (Optional) **show crypto ca certificates**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**crypto ca import** *name* **certificate** **Example:** switch(config)# crypto ca import admin-ca certificate input (cut & paste) certificate in PEM format: -----BEGIN CERTIFICATE----- MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47 glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6 Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6 Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl	Prompts you to cut and paste the identity certificate for the CA named admin-ca. The maximum number of identify certificates that you can configure on a device is 16.

	Command or Action	Purpose
	LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4 XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw E36cIZu4WsExREqxbTk8ycx7V5o= -----END CERTIFICATE-----	

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

Step 4	(Optional) **show crypto ca certificates** **Example:** `switch# show crypto ca certificates`	Displays the CA certificates.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Creating a Trust Point CA Association, on page 195

Ensuring Trust Point Configurations Persist Across Reboots

You can ensure that the trustpoint configuration persists across Cisco NX-OS device reboots.

The trust point configuration is a normal Cisco NX-OS device configuration that persists across system reboots only if you copy it explicitly to the startup configuration. The certificates, key pairs, and CRL associated with a trust point are automatically persistent if you have already copied the trust point configuration in the startup configuration. Conversely, if the trust point configuration is not copied to the startup configuration, the certificates, key pairs, and CRL associated with it are not persistent since they require the corresponding trust point configuration after a reboot. Always copy the running configuration to the startup configuration to ensure that the configured certificates, key pairs, and CRLs are persistent. Also, save the running configuration after deleting a certificate or key pair to ensure that the deletions permanent.

The certificates and CRL associated with a trust point automatically become persistent when imported (that is, without explicitly copying to the startup configuration) if the specific trust point is already saved in startup configuration.

We recommend that you create a password-protected backup of the identity certificates and save it to an external server.

Note Copying the configuration to an external server does include the certificates and key pairs.

Related Topics

Exporting Identity Information in PKCS 12 Format, on page 206

Exporting Identity Information in PKCS 12 Format

You can export the identity certificate along with the RSA key pair and CA certificate (or the entire chain in the case of a subordinate CA) of a trust point to a PKCS#12 file for backup purposes. You can import the certificate and RSA key pair to recover from a system crash on your device or when you replace the supervisor modules.

Note You can use only the bootflash:*filename* format when specifying the export URL.

Before you begin

Authenticate the CA.

Install an identity certificate.

SUMMARY STEPS

1. **configure terminal**
2. **crypto ca export** *name* **pkcs12 bootflash:***filename password*
3. **exit**
4. **copy booflash:***filename scheme***://***server***/** [*url* **/**]*filename*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**crypto ca export** *name* **pkcs12 bootflash:***filename password* **Example:** `switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123`	Exports the identity certificate and associated key pair and CA certificates for a trust point CA. The password is alphanumeric, case sensitive, and has a maximum length of 128 characters.

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

Step 4	**copy booflash:***filename scheme***://***server***/** [*url* **/**]*filename* **Example:** `switch# copy bootflash:adminid.p12 tftp:adminid.p12`	Copies the PKCS#12 format file to a remote server. For the *scheme* argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**. The *server* argument is the address or name of the remote server, and the *url* argument is the path to the source file on the remote server. The *server*, *url*, and *filename* arguments are case sensitive.

Related Topics

Generating an RSA Key Pair, on page 193
Authenticating the CA, on page 199
Installing Identity Certificates, on page 204

Importing Identity Information in PKCS 12 Format

You can import the certificate and RSA key pair to recover from a system crash on your device or when you replace the supervisor modules.

Note You can use only the bootflash:*filename* format when specifying the import URL.

Before you begin

Ensure that the trust point is empty by checking that no RSA key pair is associated with it and no CA is associated with the trust point using CA authentication.

SUMMARY STEPS

1. **copy** *scheme*:// *server*/[*url* /]*filename* **bootflash:***filename*
2. **configure terminal**
3. **crypto ca import** *name* **pksc12 bootflash:***filename*
4. **exit**
5. (Optional) **show crypto ca certificates**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**copy** *scheme*:// *server*/[*url* /]*filename* **bootflash:***filename* **Example:** `switch# copy tftp:adminid.p12 bootflash:adminid.p12`	Copies the PKCS#12 format file from the remote server. For the *scheme* argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**. The *server* argument is the address or name of the remote server, and the *url* argument is the path to the source file on the remote server. The *server*, *url*, and *filename* arguments are case sensitive.

Step 2	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 3	**crypto ca import** *name* **pksc12 bootflash:***filename* **Example:** `switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123`	Imports the identity certificate and associated key pair and CA certificates for trust point CA.

	Command or Action	Purpose

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show crypto ca certificates** **Example:** `switch# show crypto ca certificates`	Displays the CA certificates.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring a CRL

You can manually configure CRLs that you have downloaded from the trust points. The Cisco NX-OS software caches the CRLs in the device bootflash (cert-store). During the verification of a peer certificate, the Cisco NX-OS software checks the CRL from the issuing CA only if you have downloaded the CRL to the device and you have configured certificate revocation checking to use the CRL.

Before you begin

Ensure that you have enabled certificate revocation checking.

SUMMARY STEPS

1. **copy** *scheme*:[//*server*/[*url* /]]*filename* **bootflash:***filename*
2. **configure terminal**
3. **crypto ca crl request** *name* **bootflash:***filename*
4. **exit**
5. (Optional) **show crypto ca crl** *name*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**copy** *scheme*:[//*server*/[*url* /]]*filename* **bootflash:***filename* **Example:** `switch# copy tftp:adminca.crl bootflash:adminca.crl`	Downloads the CRL from a remote server. For the *scheme* argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**. The *server* argument is the address or name of the remote server, and the *url* argument is the path to the source file on the remote server. The *server*, *url*, and *filename* arguments are case sensitive.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
Step 3	**crypto ca crl request** *name* **bootflash:***filename* **Example:** `switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl`	Configures or replaces the current CRL with the one specified in the file.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show crypto ca crl** *name* **Example:** `switch# show crypto ca crl admin-ca`	Displays the CA CRL information.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Deleting Certificates from the CA Configuration

You can delete the identity certificates and CA certificates that are configured in a trust point. You must first delete the identity certificate, followed by the CA certificates. After deleting the identity certificate, you can disassociate the RSA key pair from a trust point. You must delete certificates to remove expired or revoked certificates, certificates that have compromised (or suspected to be compromised) key pairs, or CAs that are no longer trusted.

SUMMARY STEPS

1. **configure terminal**
2. **crypto ca trustpoint** *name*
3. **delete ca-certificate**
4. **delete certificate** [**force**]
5. **exit**
6. (Optional) **show crypto ca certificates** [*name*]
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**crypto ca trustpoint** *name*
	Example:
	`switch(config)# crypto ca trustpoint admin-ca`
	`switch(config-trustpoint)#`
		Specifies a trust point CA and enters trust point configuration mode.

Step 3	**delete ca-certificate** **Example:** `switch(config-trustpoint)# delete ca-certificate`	Deletes the CA certificate or certificate chain.
Step 4	**delete certificate** [**force**] **Example:** `switch(config-trustpoint)# delete certificate`	Deletes the identity certificate. You must use the **force** option if the identity certificate you want to delete is the last certificate in a certificate chain or only identity certificate in the device. This requirement ensures that you do not mistakenly delete the last certificate in a certificate chain or only the identity certificate and leave the applications (such as SSH) without a certificate to use.

Step 5	**exit**
	Example:
	`switch(config-trustpoint)# exit`
	`switch(config)#`
		Exits trust point configuration mode.

Step 6	(Optional) **show crypto ca certificates** [*name*] **Example:** `switch(config)# show crypto ca certificates admin-ca`	Displays the CA certificate information.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Deleting RSA Key Pairs from a Cisco NX-OS Device

You can delete the RSA key pairs from a Cisco NX-OS device if you believe the RSA key pairs were compromised in some way and should no longer be used.

Note After you delete RSA key pairs from a device, ask the CA administrator to revoke your device's certificates at the CA. You must supply the challenge password that you created when you originally requested the certificates.

SUMMARY STEPS

1. **configure terminal**
2. **crypto key zeroize rsa** *label*

3. **exit**
4. (Optional) **show crypto key mypubkey rsa**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**crypto key zeroize rsa** *label* **Example:** `switch(config)# crypto key zeroize rsa MyKey`	Deletes the RSA key pair.

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

Step 4	(Optional) **show crypto key mypubkey rsa** **Example:** `switch# show crypto key mypubkey rsa`	Displays the RSA key pair configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Generating Certificate Requests, on page 202

Verifying the PKI Configuration

To display PKI configuration information, perform one of the following tasks:

Command	Purpose
show crypto key mypubkey rsa	Displays information about the RSA public keys generated on the Cisco NX-OS device.
show crypto ca certificates	Displays information about CA and identity certificates.
show crypto ca crl	Displays information about CA CRLs.

Command	Purpose
show crypto ca certstore	Displays the cert-store configuration.
show crypto ca remote-certstore	Displays the remote cert-store configuration.
show crypto certificatemap	Displays the certificate mapping filters.
show crypto ssh-auth-map	Displays the mapping filters configured for SSH authorization.
show crypto ca trustpoints	Displays information about CA trust points.

Configuration Examples for PKI

This section shows examples of the tasks that you can use to configure certificates and CRLs on Cisco NX-OS devices using a Microsoft Windows Certificate server.

Note You can use any type of certificate server to generate digital certificates. You are not limited to using the Microsoft Windows Certificate server.

Configuring Certificates on a Cisco NX-OS Device

To configure certificates on a Cisco NX-OS device, follow these steps:

Step 1 Configure the device FQDN.

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# hostname Device-1
Device-1(config)#
```

Step 2 Configure the DNS domain name for the device.

```
Device-1(config)# ip domain-name cisco.com
```

Step 3 Create a trust point.

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key:
revokation methods:  crl
```

Step 4 Create an RSA key pair for the device.

```
Device-1(config)# crypto key generate rsa label myKey exportable modulus 1024
Device-1(config)# show crypto key mypubkey rsa
key label: myKey
key size: 1024
exportable: yes
```

Step 5 Associate the RSA key pair to the trust point.

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# rsakeypair myKey
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key: myKey
revokation methods:  crl
```

Step 6 Download the CA certificate from the Microsoft Certificate Service web interface.

Step 7 Authenticate the CA that you want to enroll to the trust point.

```
Device-1(config)# crypto ca authenticate myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]:y

Device-1(config)# show crypto ca certificates
Trustpoint: myCA
CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May  3 22:46:37 2005 GMT
notAfter=May  3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

Step 8 Generate a request certificate to use to enroll with a trust point.

```
Device-1(config)# crypto ca enroll myCA
 Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password: nbv123
 The subject name in the certificate will be: Device-1.cisco.com
 Include the switch serial number in the subject name? [yes/no]: no
 Include an IP address in the subject name [yes/no]: yes
ip address: 10.10.1.1
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

Step 9 Request an identity certificate from the Microsoft Certificate Service web interface.

Step 10 Import the identity certificate.

```
Device-1(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
Device-1(config)# exit
Device-1#
```

Step 11 Verify the certificate configuration.

Step 12 Save the certificate configuration to the startup configuration.

Related Topics

Downloading a CA Certificate, on page 216
Requesting an Identity Certificate, on page 219

Configuring the Cert-Store and Certificate Mapping Filters

To configure a remote cert-store for certificate authentication and to configure certificate mapping filters, follow these steps:

SUMMARY STEPS

1. Specify the remote cert-store for certificate authentication.
2. Display the cert-store configuration.
3. Configure the LDAP server group to be used while communicating with LDAP.
4. Configure the refresh time to update the certificate revocation list (CRL) from the remote cert-store.
5. Displays the remote cert-store configuration.
6. Create a new filter map.
7. Configure certificate mapping filters within the filter map.
8. Configure a certificate mapping filter for SSH.
9. Display the certificate mapping filters.
10. Save the certificate configuration to the startup configuration.

DETAILED STEPS

Step 1 Specify the remote cert-store for certificate authentication.

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# crypto ca lookup remote
switch(config)#
```

Step 2 Display the cert-store configuration.

```
switch(config)# show crypto ca certstore
```

Step 3 Configure the LDAP server group to be used while communicating with LDAP.

```
switch(config)# crypto ca remote ldap server-group group1
```

Step 4 Configure the refresh time to update the certificate revocation list (CRL) from the remote cert-store.

```
switch(config)# crypto ca remote ldap crl-refresh-time 10
```

Step 5 Displays the remote cert-store configuration.

```
switch(config)# show crypto ca remote-certstore
```

Step 6 Create a new filter map.

```
switch(config)# crypto certificatemap mapname filtermap1
```

Step 7 Configure certificate mapping filters within the filter map.

```
switch(config-certmap-filter)# filter subject-name cn=jsmith,ou=PKI,o=Acme,c=US
switch(config-certmap-filter)# filter altname-email jsmith@acme.com
switch(config-certmap-filter)# exit
switch(config)#
```

Step 8 Configure a certificate mapping filter for SSH.

```
switch(config)# crypto cert ssh-authorize default map filtermap1
```

Step 9 Display the certificate mapping filters.

```
switch(config)# show crypto certificatemap
switch(config)# show crypto ssh-auth-map
```

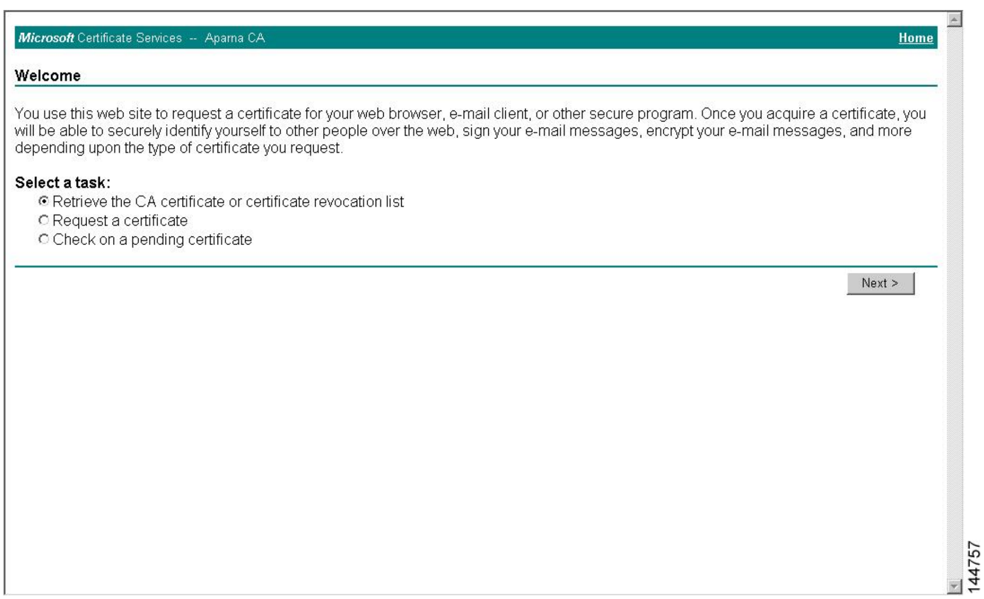
Step 10 Save the certificate configuration to the startup configuration.

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

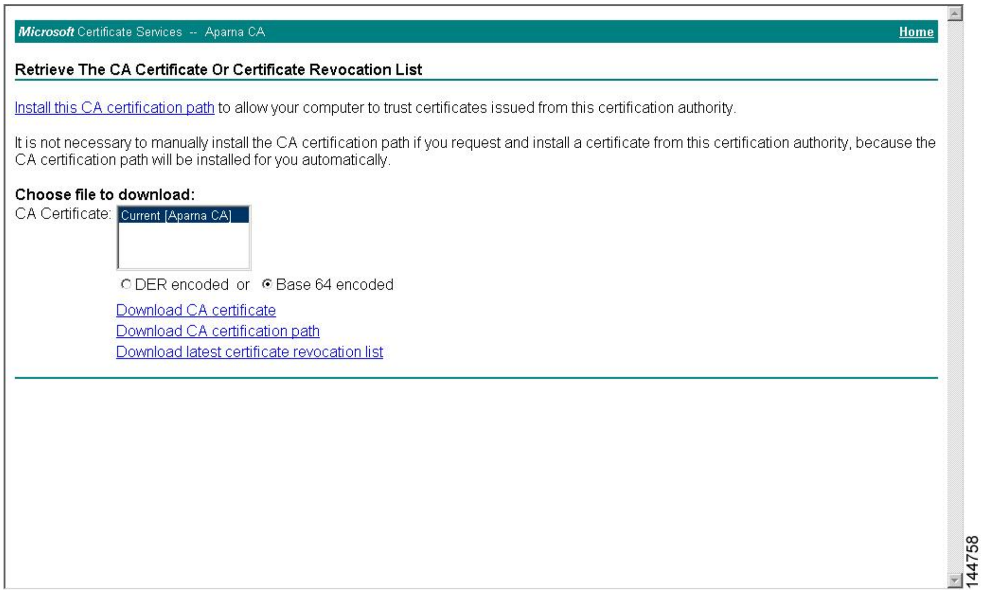
Downloading a CA Certificate

To download a CA certificate from the Microsoft Certificate Services web interface, follow these steps:

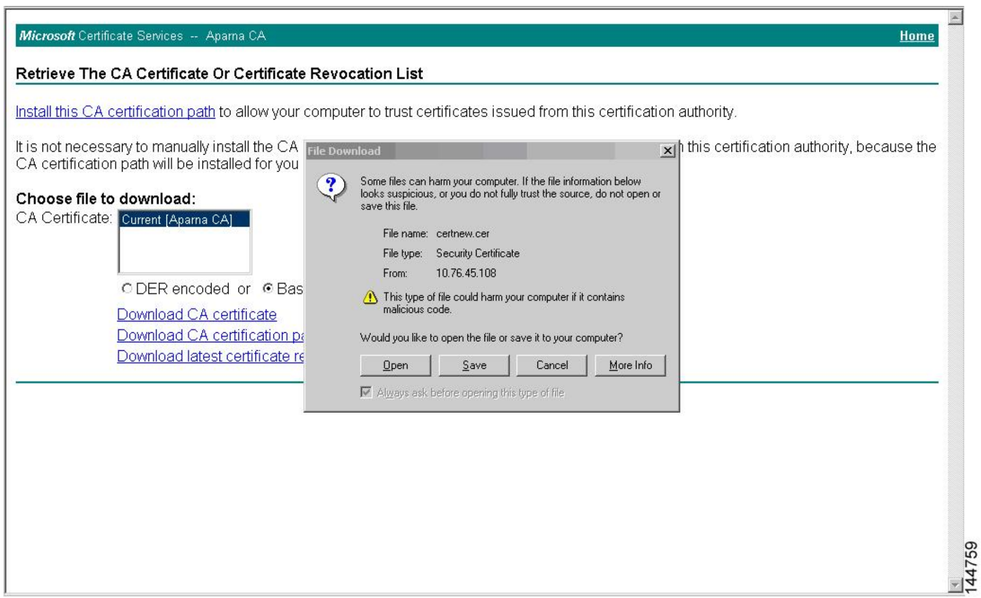
Step 1 From the Microsoft Certificate Services web interface, click **Retrieve the CA certificate or certificate revocation task** and click **Next**.



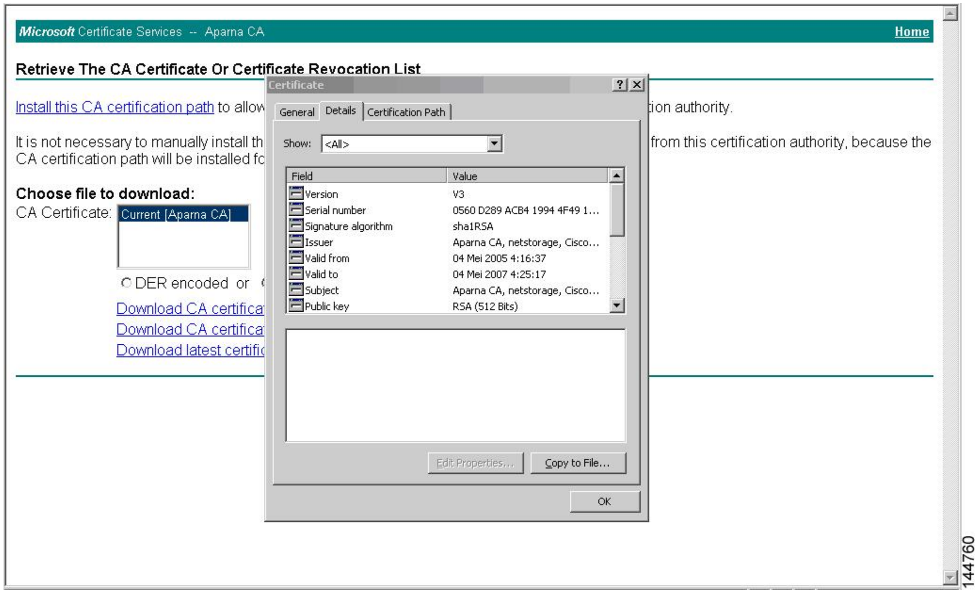
Step 2 From the display list, choose the CA certificate file to download from the displayed list. Then click **Base 64 encoded** and click **Download CA certificate**.



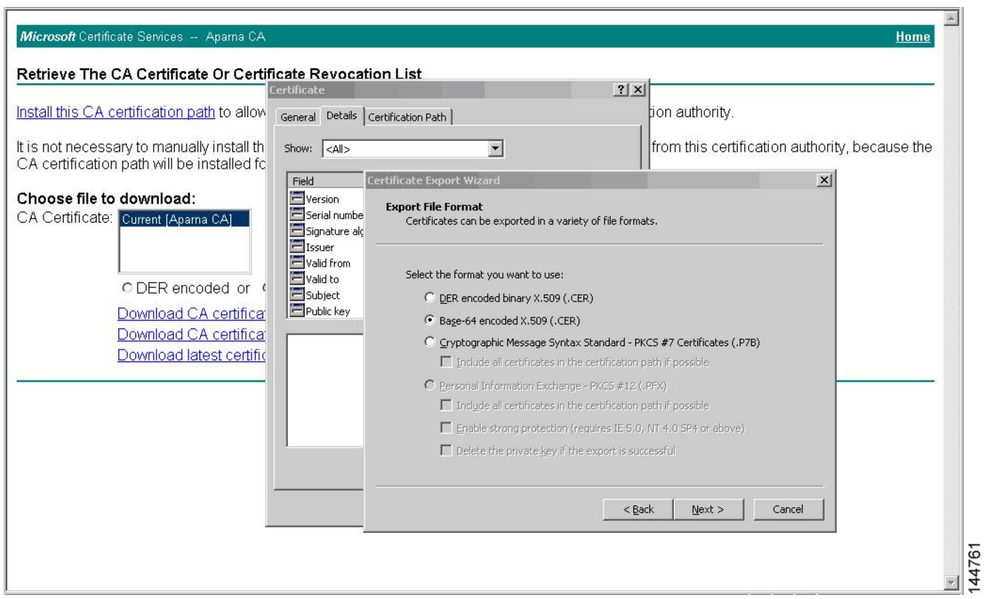
Step 3 Click **Open** in the File Download dialog box.



Step 4 In the Certificate dialog box, click **Copy to File** and click **OK**.



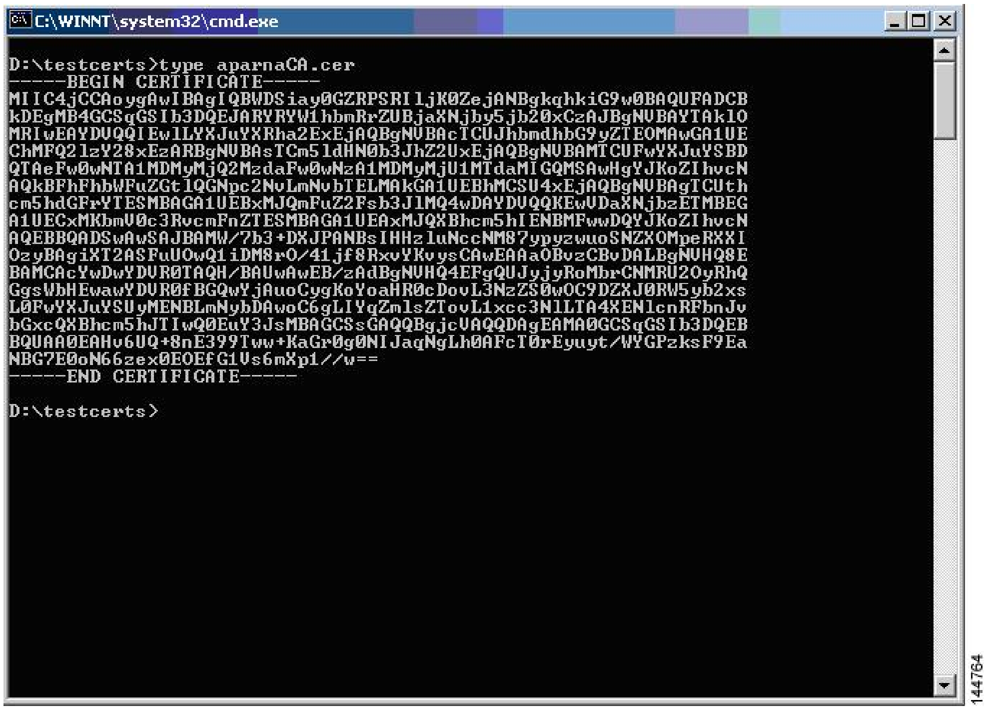
Step 5 From the Certificate Export Wizard dialog box, choose the **Base-64 encoded X.509 (CER)** and click **Next**.



Step 6 In the File name: text box on the Certificate Export Wizard dialog box, enter the destination file name and click **Next**.

Step 7 In the Certificate Export Wizard dialog box, click **Finish**.

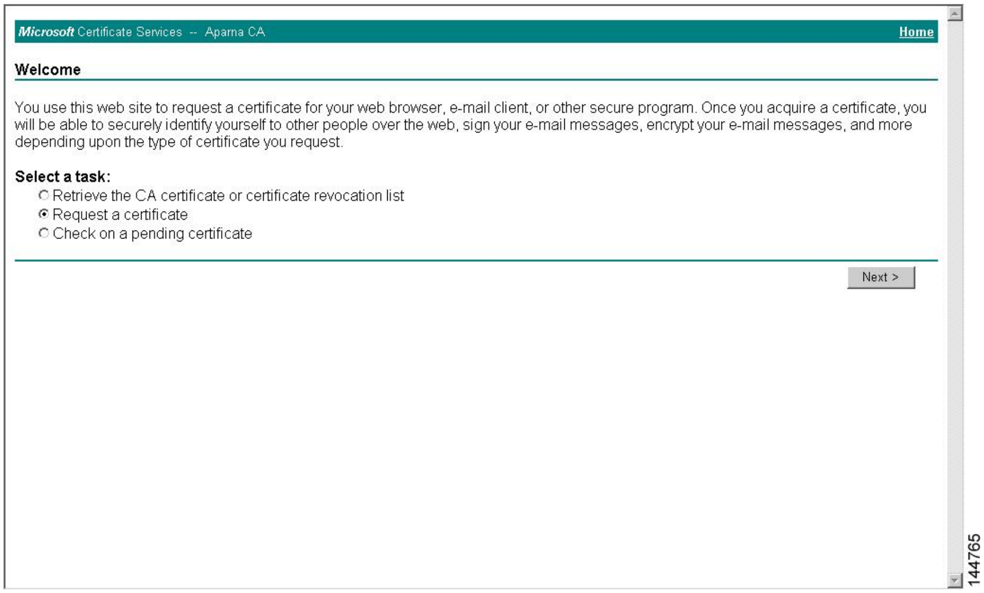
Step 8 Enter the Microsoft Windows **type** command to display the CA certificate stored in Base-64 (PEM) format.



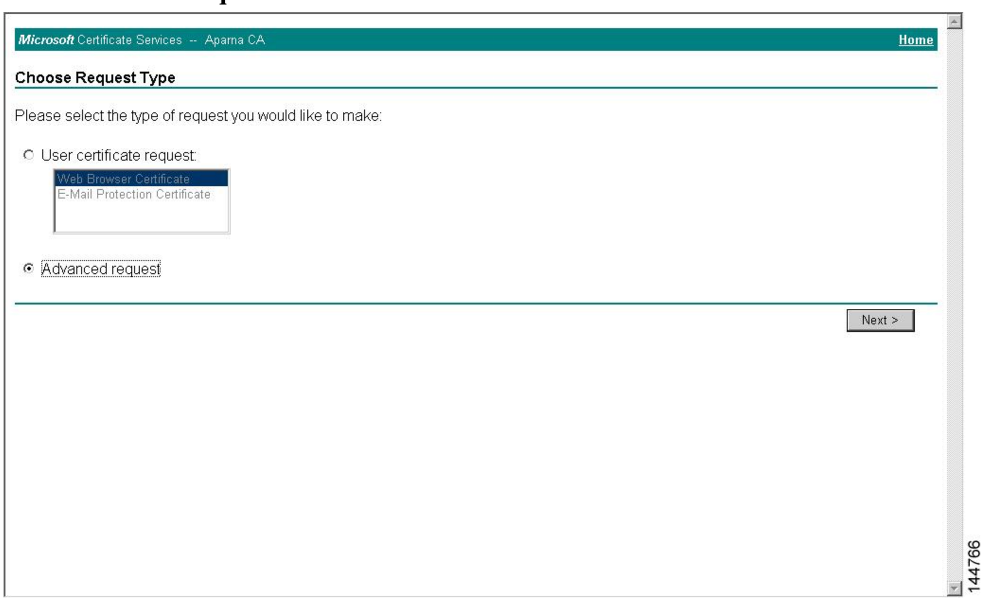
Requesting an Identity Certificate

To request an identify certificate from a Microsoft Certificate server using a PKCS#12 certificate signing request (CRS), follow these steps:

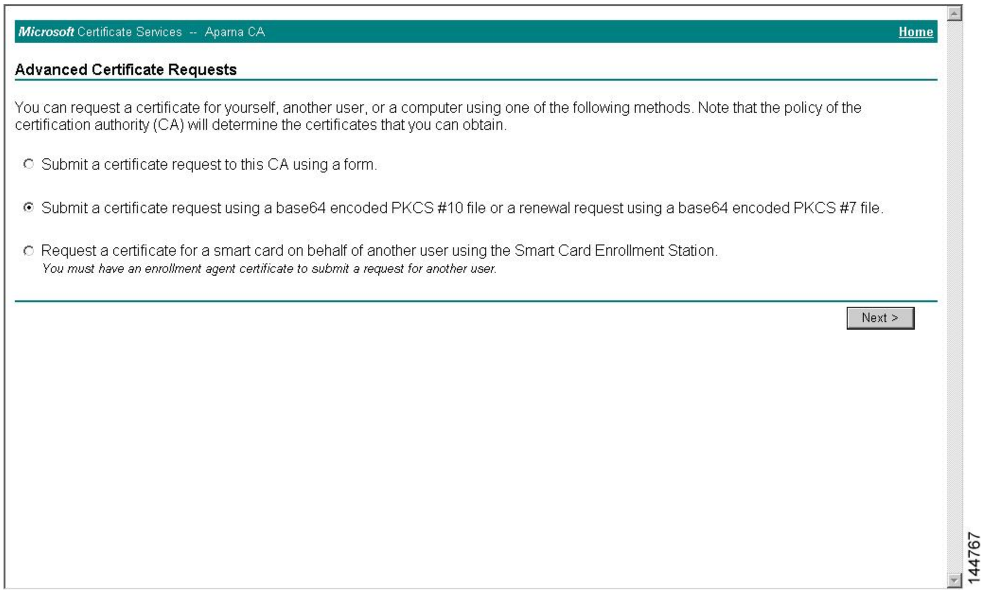
Step 1 From the Microsoft Certificate Services web interface, click **Request a certificate** and click **Next**.



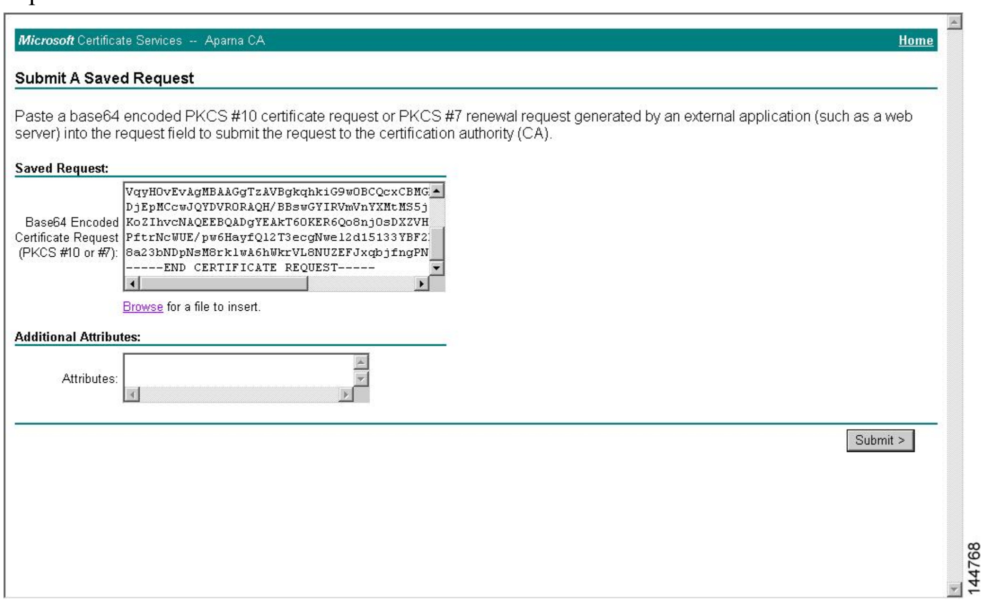
Step 2 Click **Advanced request** and click **Next**.



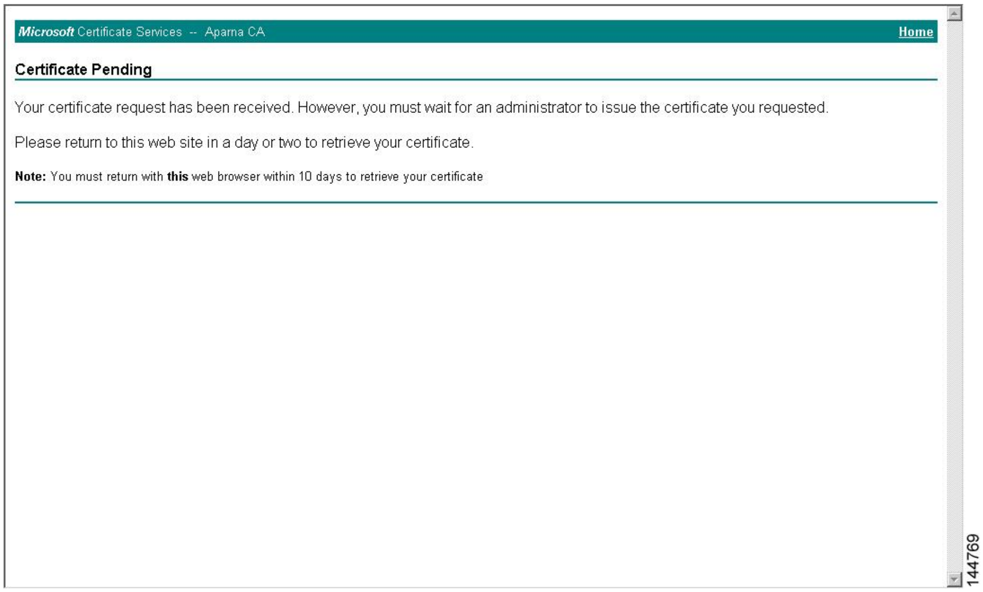
Step 3 Click **Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file** and click **Next**.



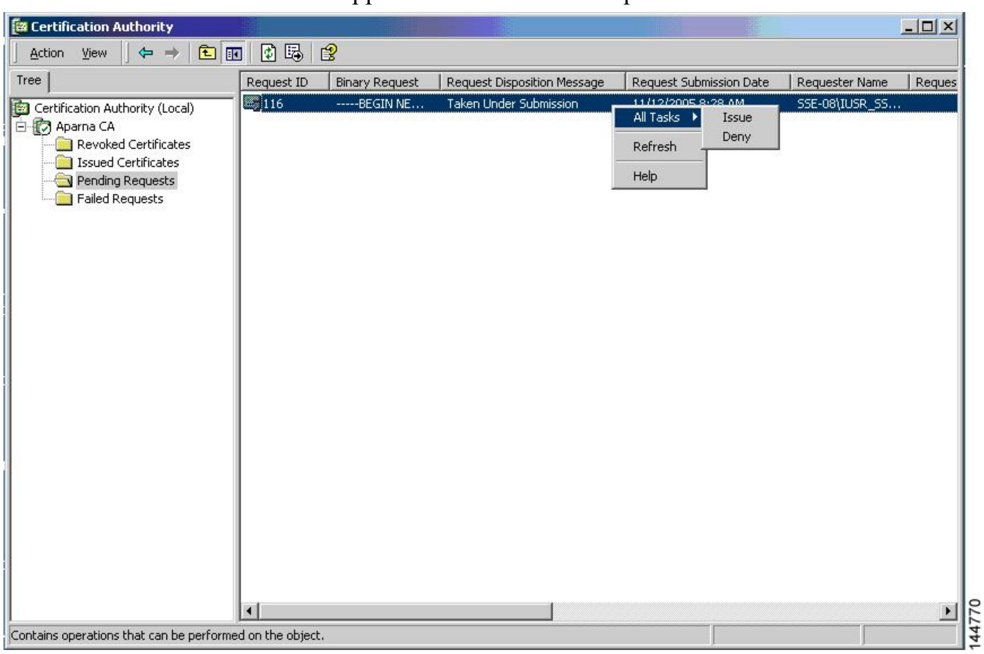
Step 4 In the Saved Request text box, paste the base64 PKCS#10 certificate request and click **Next**. The certificate request is copied from the Cisco NX-OS device console.



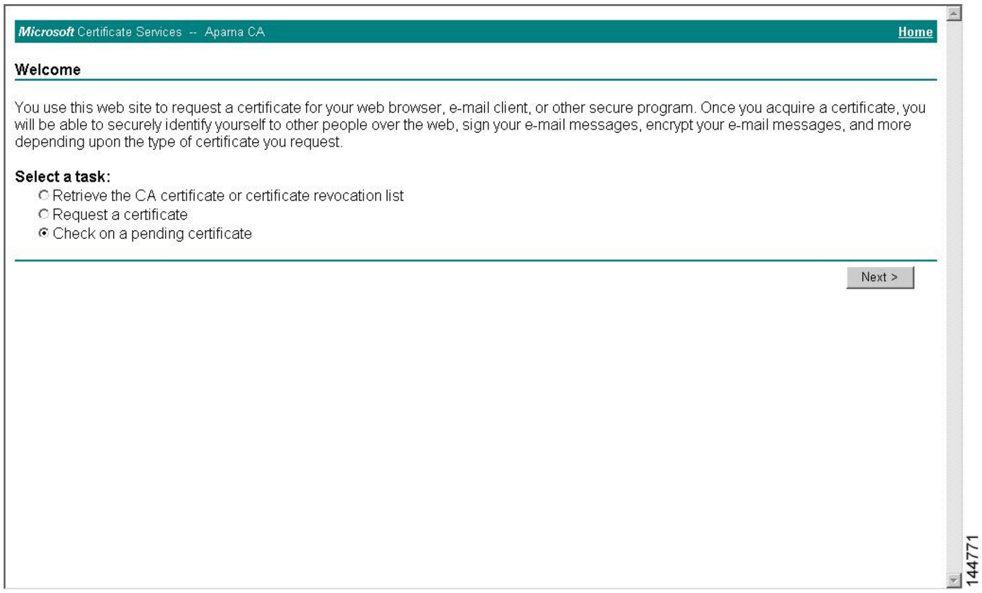
Step 5 Wait one or two days until the certificate is issued by the CA administrator.



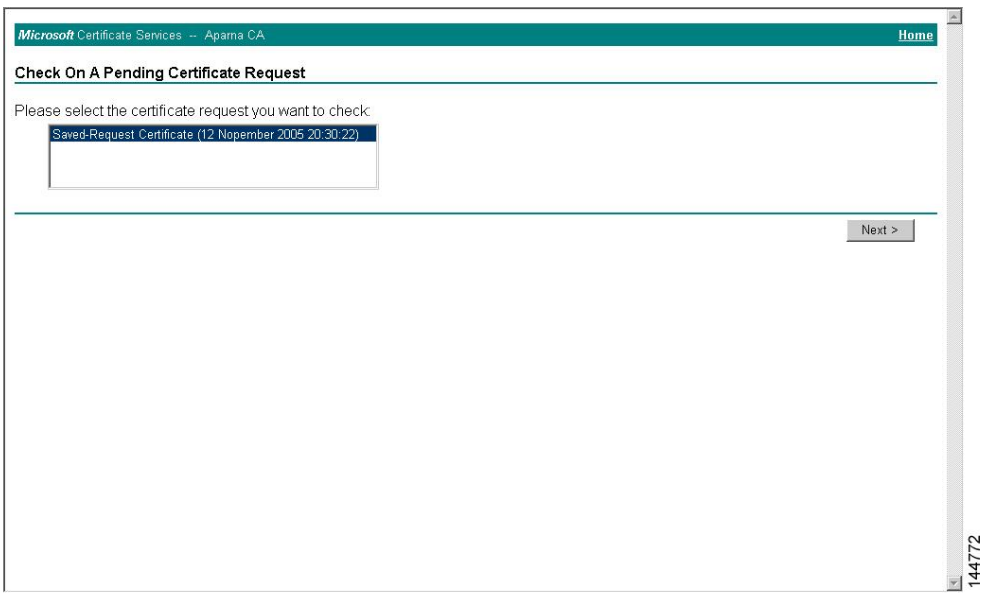
Step 6 Note that the CA administrator approves the certificate request.



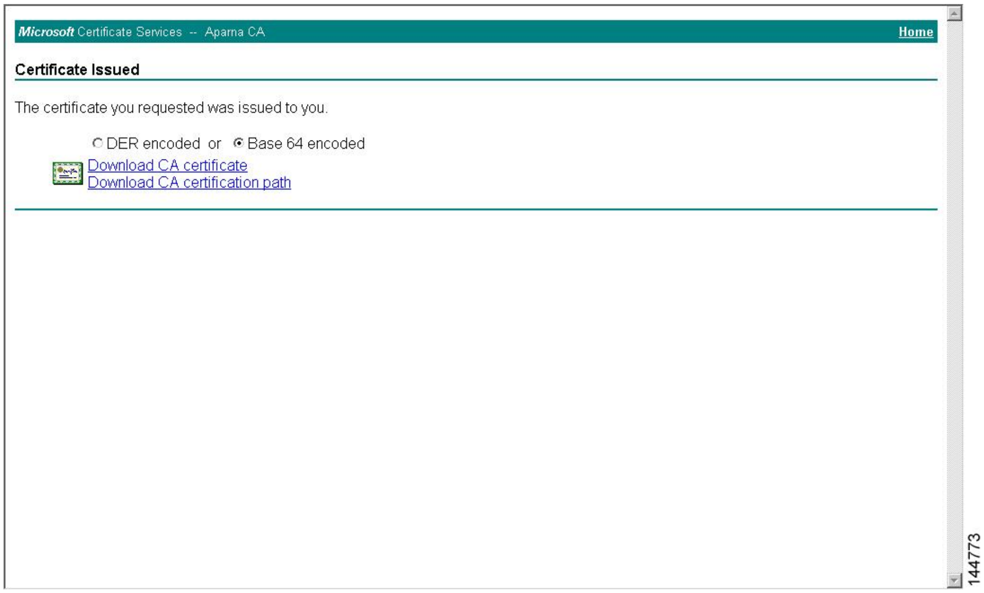
Step 7 From the Microsoft Certificate Services web interface, click **Check on a pending certificate** and click **Next**.



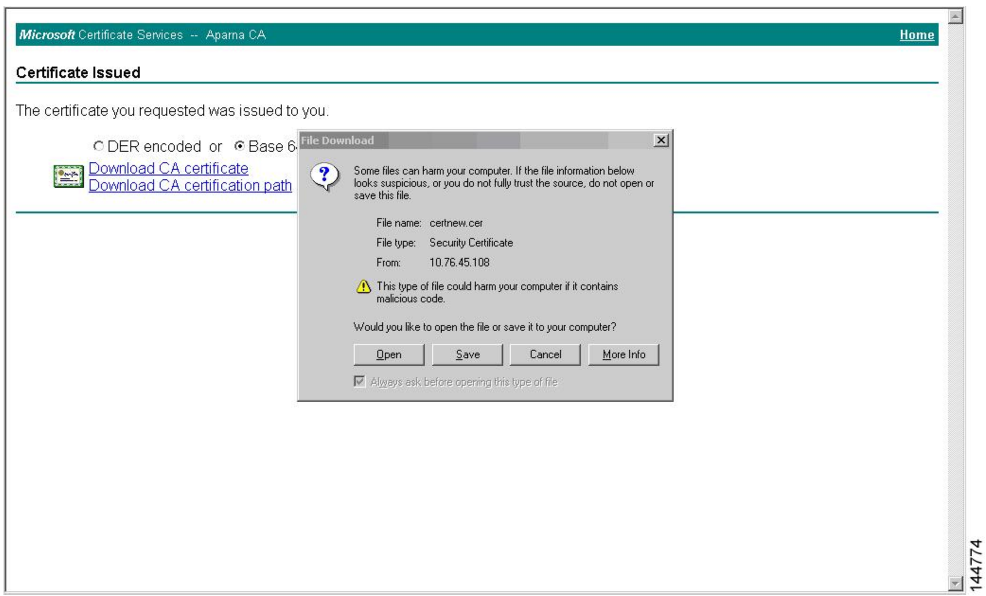
Step 8 Choose the certificate request that you want to check and click **Next**.



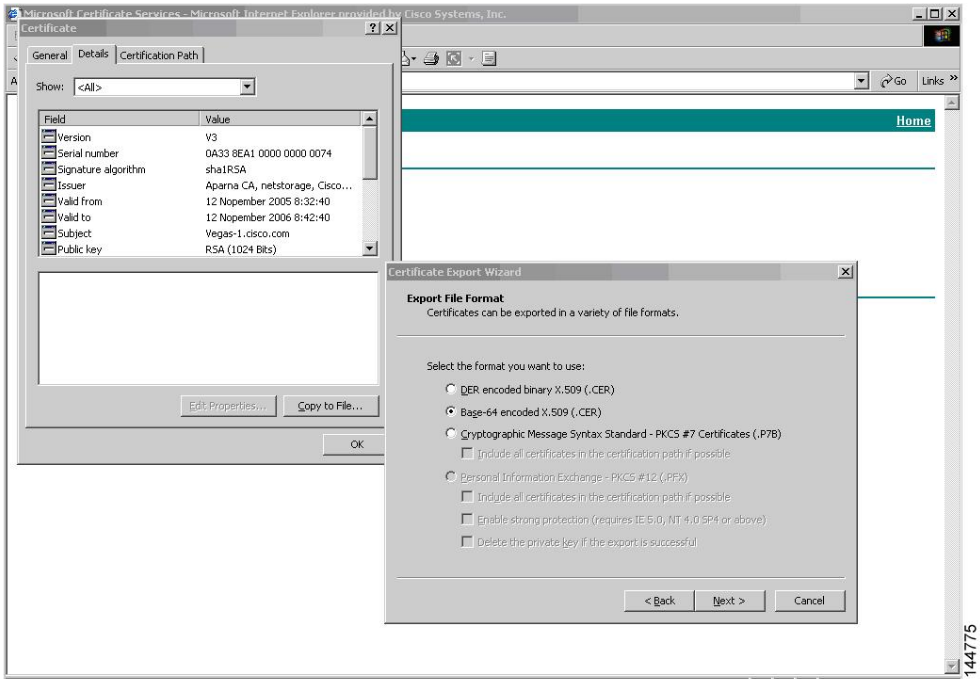
Step 9 Click **Base 64 encoded** and click **Download CA certificate**.



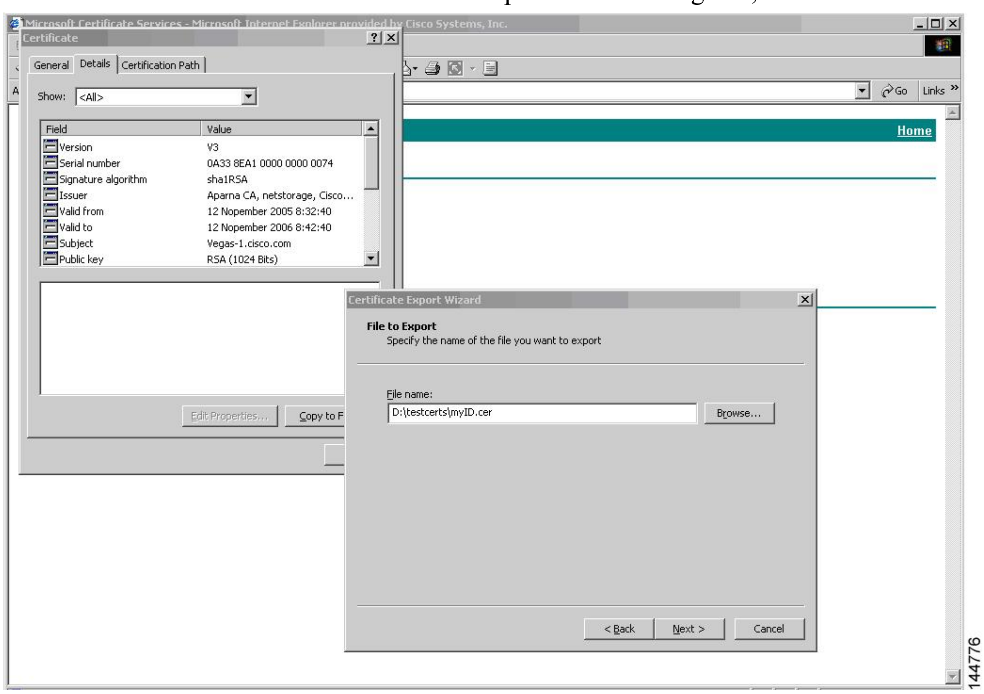
Step 10 In the File Download dialog box, click **Open**.



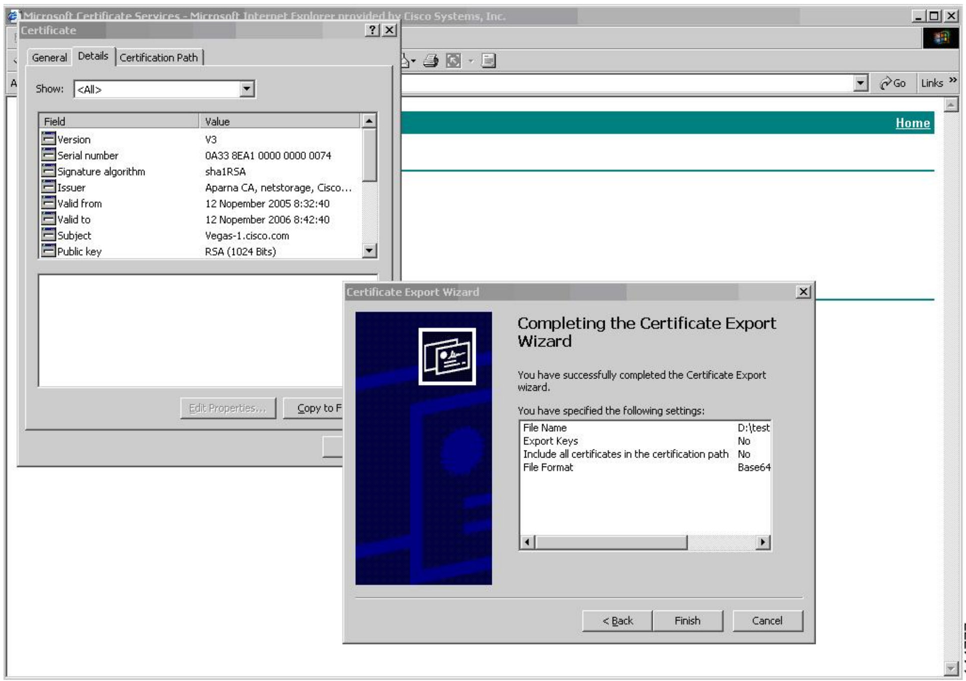
Step 11 In the Certificate box, click **Details** tab and click **Copy to File...**. In the Certificate Export Dialog box, click **Base-64 encoded X.509 (.CER)**, and click **Next**.



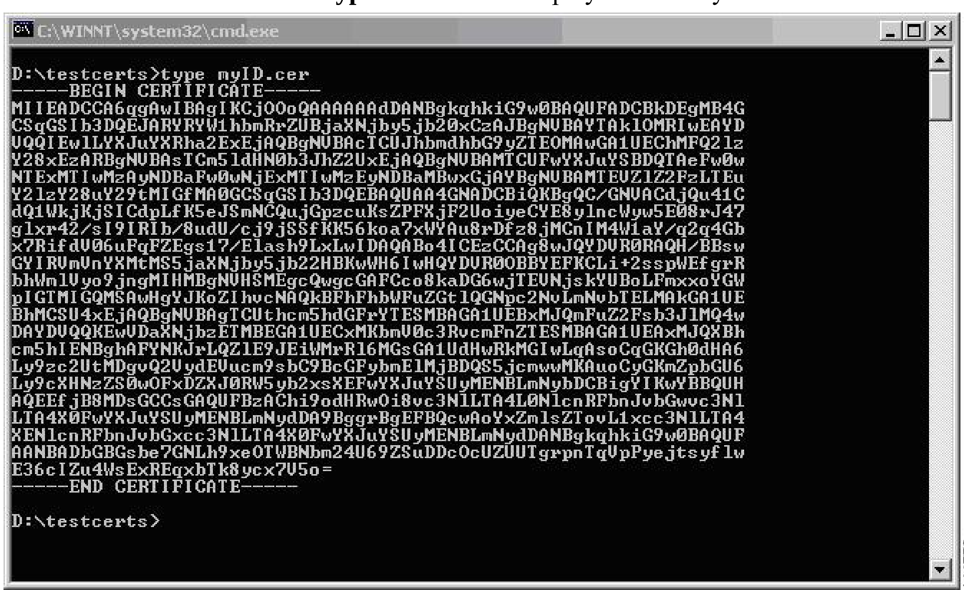
Step 12 In the File name: text box on the Certificate Export Wizard dialog box, enter the destination file name and click **Next**.



Step 13 Click **Finish**.



Step 14 Enter the Microsoft Windows **type** command to display the identity certificate in base64-encoded format.



Related Topics

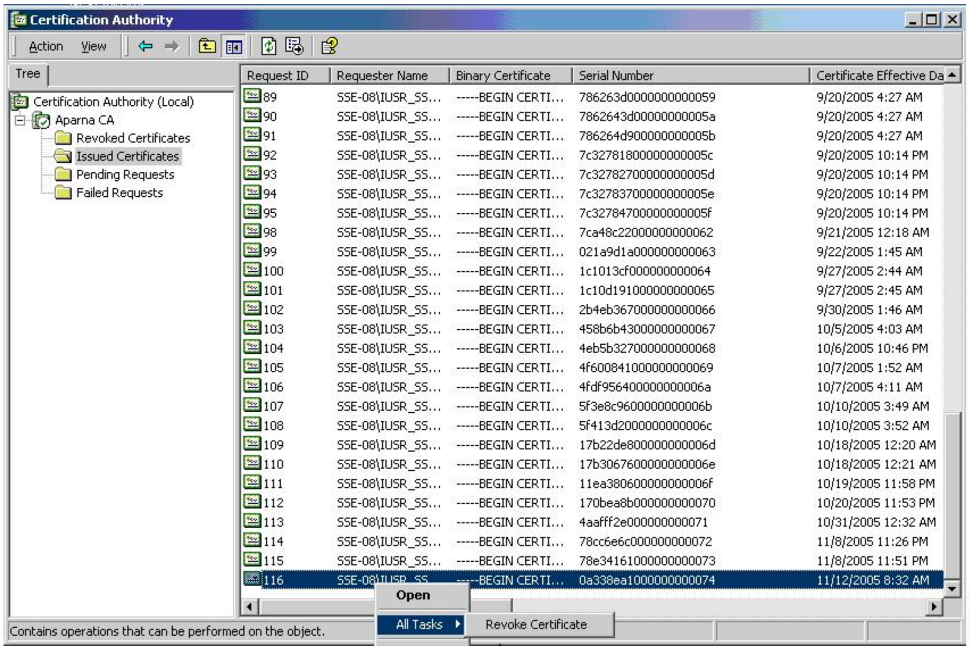
Generating Certificate Requests, on page 202
Configuring Certificates on a Cisco NX-OS Device, on page 212

Revoking a Certificate

To revoke a certificate using the Microsoft CA administrator program, follow these steps:

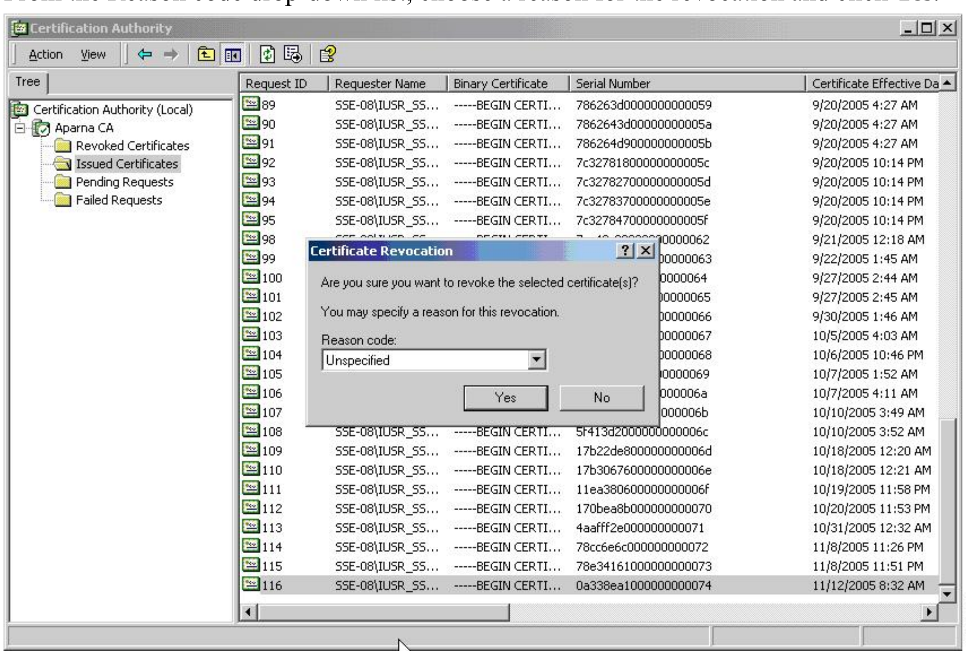
Step 1 From the Certification Authority tree, click **Issued Certificates** folder. From the list, right-click the certificate that you want to revoke.

Step 2 Choose **All Tasks** > **Revoke Certificate**.



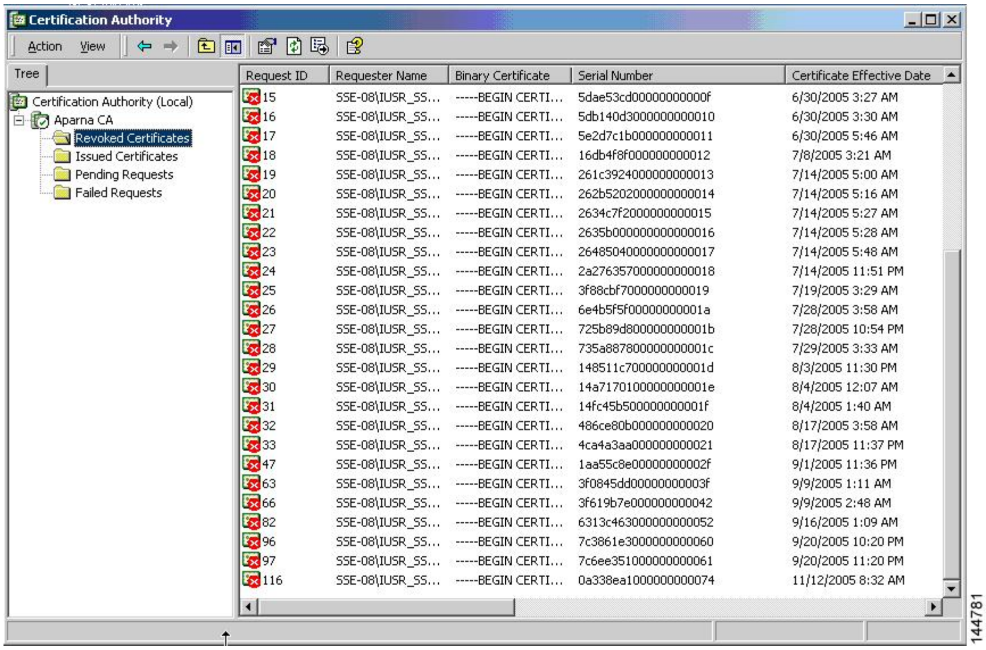
144779

Step 3 From the Reason code drop-down list, choose a reason for the revocation and click **Yes**.



144780

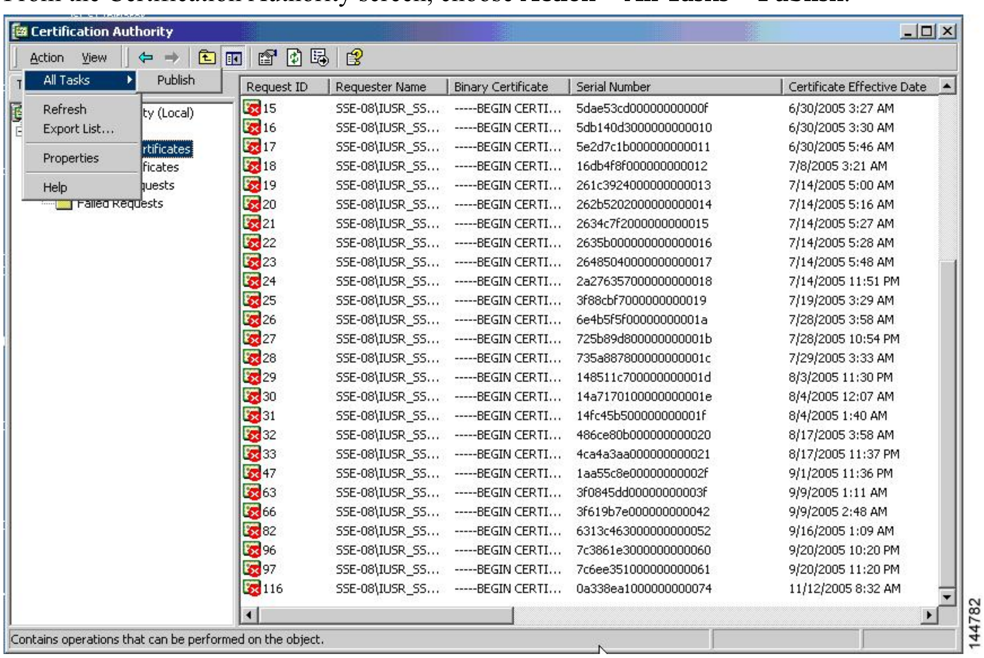
Step 4 Click the **Revoked Certificates** folder to list and verify the certificate revocation.



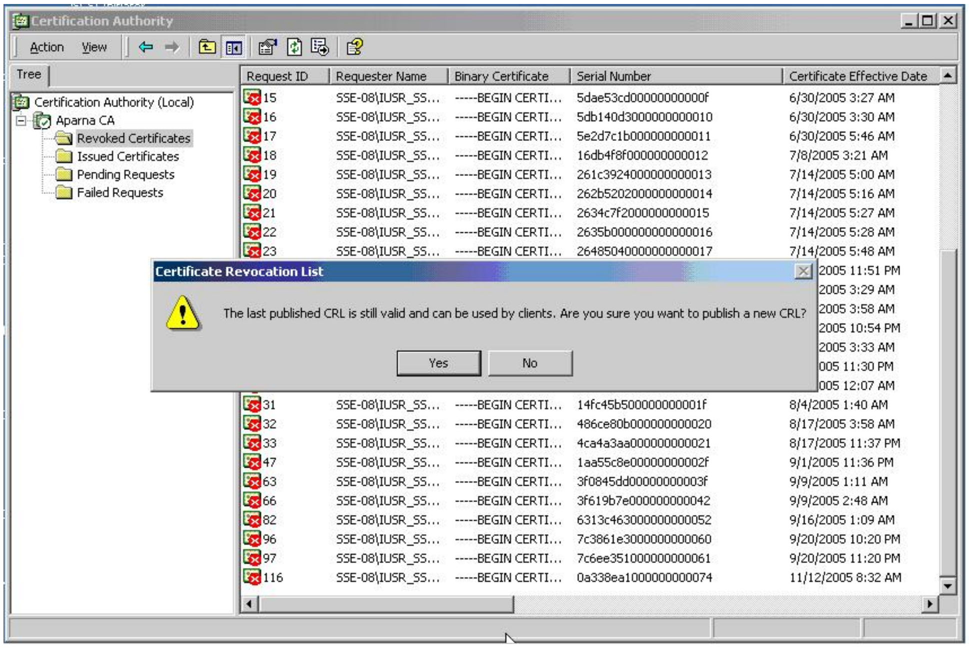
Generating and Publishing the CRL

To generate and publish the CRL using the Microsoft CA administrator program, follow these steps:

Step 1 From the Certification Authority screen, choose **Action** > **All Tasks** > **Publish**.



Step 2 In the Certificate Revocation List dialog box, click **Yes** to publish the latest CRL.

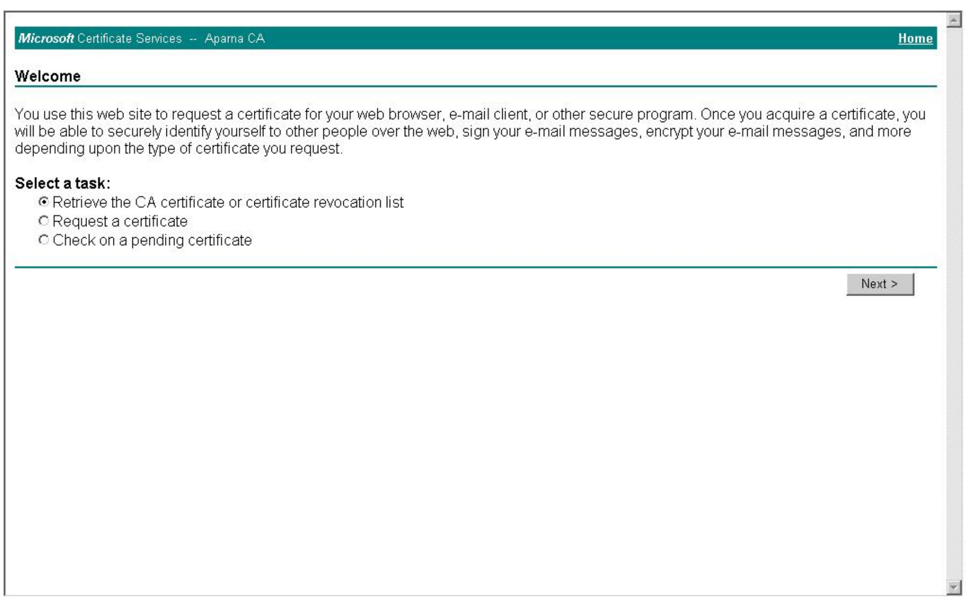


144783

Downloading the CRL

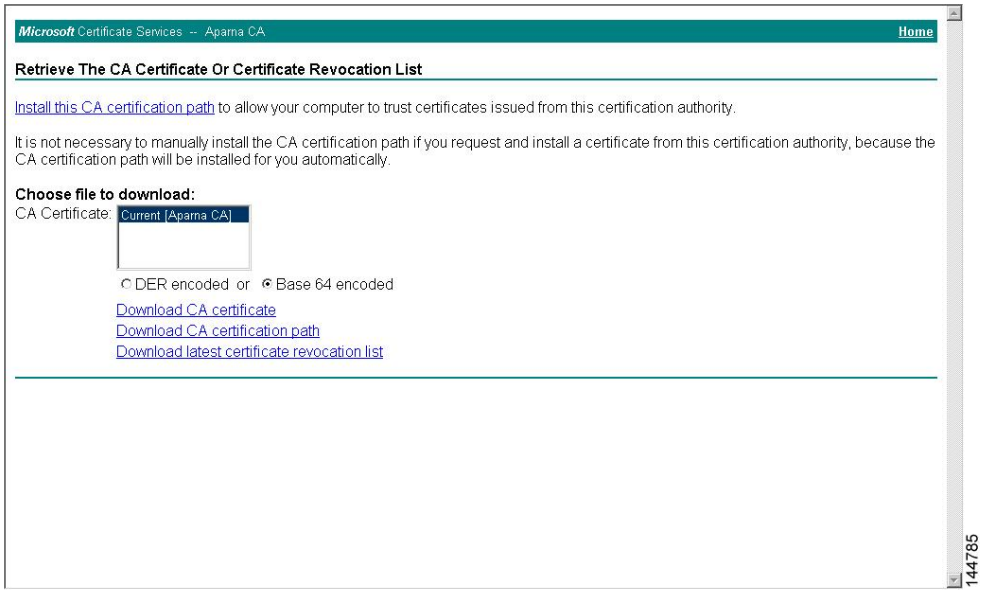
To download the CRL from the Microsoft CA website, follow these steps:

Step 1 From the Microsoft Certificate Services web interface, click **Retrieve the CA certificate or certificate revocation list** and click **Next**.

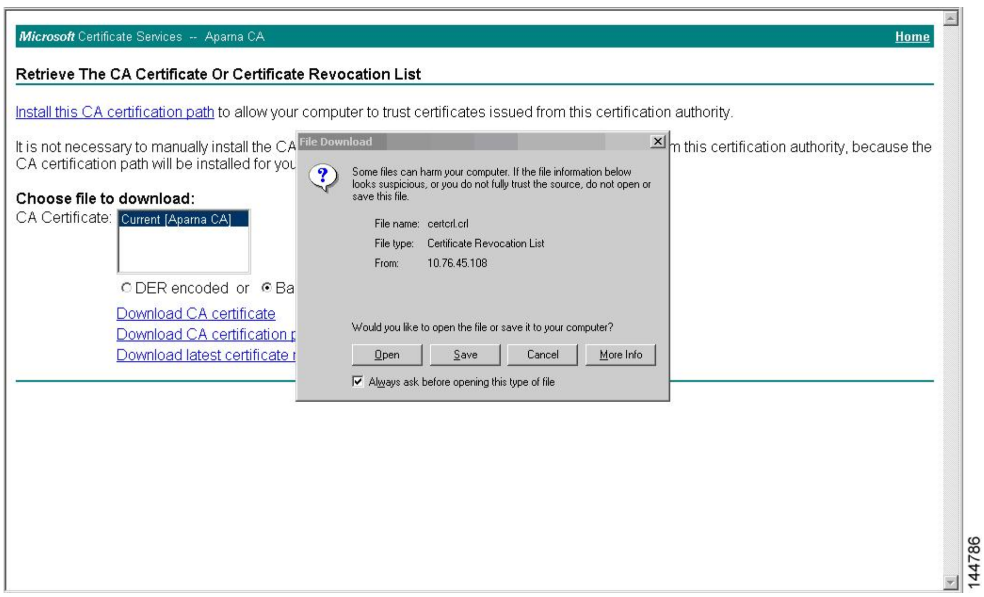


144784

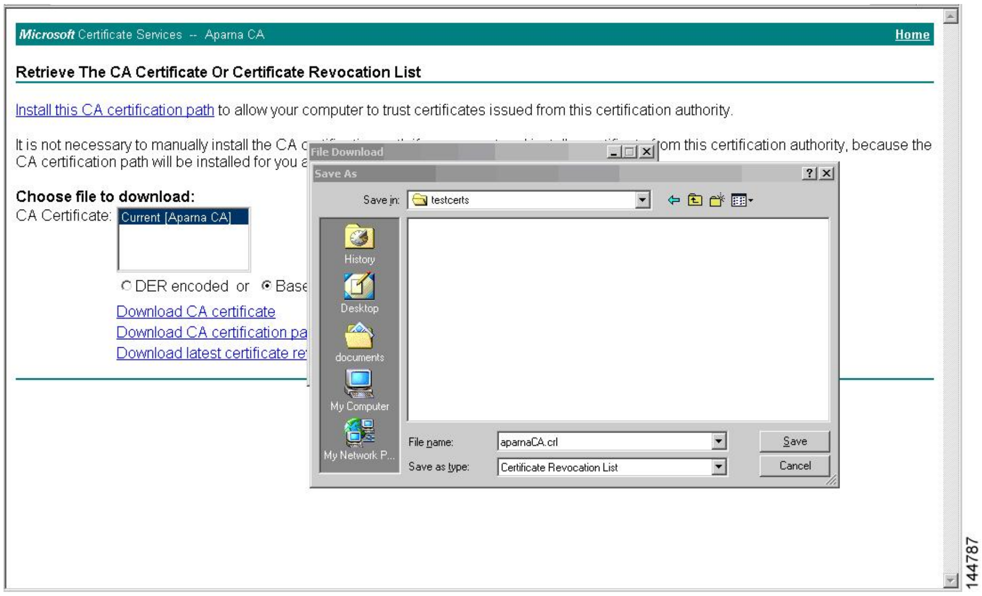
Step 2 Click **Download latest certificate revocation list**.



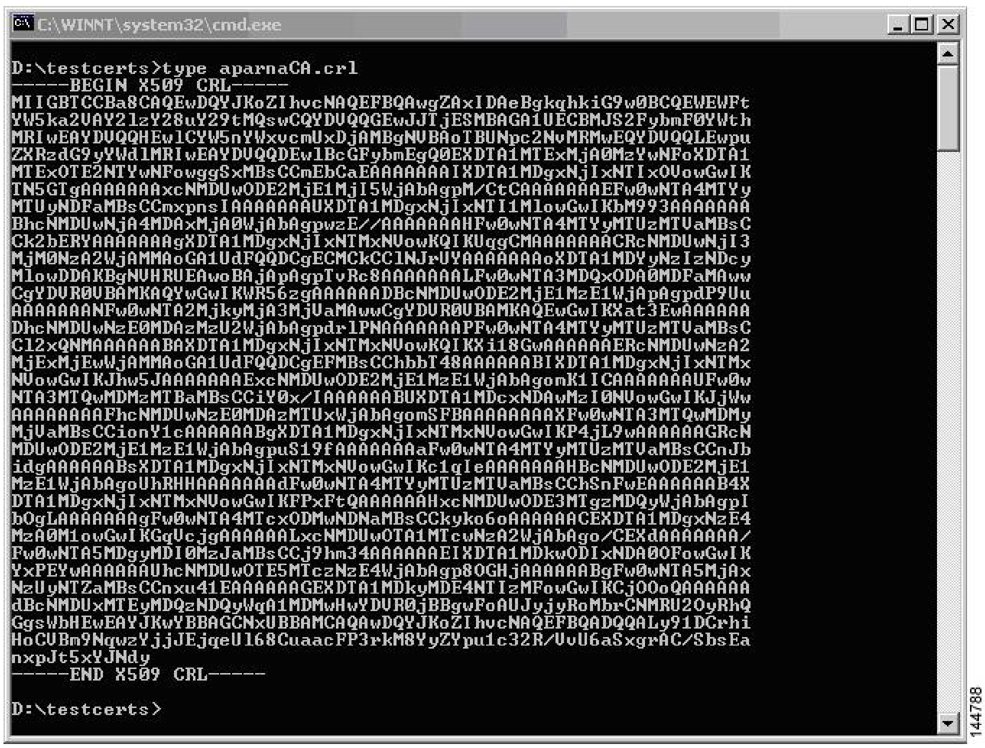
Step 3 In the File Download dialog box, click **Save**.



Step 4 In the Save As dialog box, enter the destination file name and click **Save**.



Step 5 Enter the Microsoft Windows **type** command to display the CRL.



Related Topics

Configuring Certificate Revocation Checking Methods, on page 201

Importing the CRL

To import the CRL to the trust point corresponding to the CA, follow these steps:

Step 1 Copy the CRL file to the Cisco NX-OS device bootflash.

```
Device-1# copy tftp:apranaCA.crl bootflash:aparnaCA.crl
```

Step 2 Configure the CRL.

```
Device-1# configure terminal
Device-1(config)# crypto ca crl request myCA bootflash:aparnaCA.crl
Device-1(config)#
```

Step 3 Display the contents of the CRL.

```
Device-1(config)# show crypto ca crl myCA
Trustpoint: myCA
CRL:
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /emailAddress=admin@yourcompany.com/C=IN/ST=Karnatak
Yourcompany/OU=netstorage/CN=Aparna CA
        Last Update: Nov 12 04:36:04 2005 GMT
        Next Update: Nov 19 16:56:04 2005 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
            keyid:27:28:F2:46:83:1B:AC:23:4C:45:4D:8E:C9:18:50:1
            1.3.6.1.4.1.311.21.1:
                ...
Revoked Certificates:
    Serial Number: 611B09A1000000000002
        Revocation Date: Aug 16 21:52:19 2005 GMT
Serial Number: 4CDE464E000000000003
        Revocation Date: Aug 16 21:52:29 2005 GMT
    Serial Number: 4CFC2B42000000000004
        Revocation Date: Aug 16 21:52:41 2005 GMT
    Serial Number: 6C699EC2000000000005
        Revocation Date: Aug 16 21:52:52 2005 GMT
    Serial Number: 6CCF7DDC000000000006
        Revocation Date: Jun  8 00:12:04 2005 GMT
    Serial Number: 70CC4FFF000000000007
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 4D9B1116000000000008
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 52A80230000000000009
        Revocation Date: Jun 27 23:47:06 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            CA Compromise
Serial Number: 5349AD460000000000A
        Revocation Date: Jun 27 23:47:22 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            CA Compromise
Serial Number: 53BD173C00000000000B
        Revocation Date: Jul  4 18:04:01 2005 GMT
```

```
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Certificate Hold
Serial Number: 591E7ACE00000000000C
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5D3FD52E00000000000D
        Revocation Date: Jun 29 22:07:25 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Key Compromise
Serial Number: 5DAB771300000000000E
        Revocation Date: Jul 14 00:33:56 2005 GMT
    Serial Number: 5DAE53CD00000000000F
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5DB140D3000000000010
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5E2D7C1B000000000011
        Revocation Date: Jul  6 21:12:10 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Cessation Of Operation
Serial Number: 16DB4F8F000000000012
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 261C3924000000000013
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 262B5202000000000014
        Revocation Date: Jul 14 00:33:10 2005 GMT
    Serial Number: 2634C7F2000000000015
        Revocation Date: Jul 14 00:32:45 2005 GMT
    Serial Number: 2635B000000000000016
        Revocation Date: Jul 14 00:31:51 2005 GMT
    Serial Number: 26485040000000000017
        Revocation Date: Jul 14 00:32:25 2005 GMT
    Serial Number: 2A276357000000000018
Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 3F88CBF7000000000019
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 6E4B5F5F00000000001A
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 725B89D800000000001B
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 735A887800000000001C
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 148511C700000000001D
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 14A7170100000000001E
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 14FC45B500000000001F
        Revocation Date: Aug 17 18:30:42 2005 GMT
    Serial Number: 486CE80B000000000020
        Revocation Date: Aug 17 18:30:43 2005 GMT
    Serial Number: 4CA4A3AA000000000021
        Revocation Date: Aug 17 18:30:43 2005 GMT
    Serial Number: 1AA55C8E00000000002F
        Revocation Date: Sep  5 17:07:06 2005 GMT
    Serial Number: 3F0845DD00000000003F
        Revocation Date: Sep  8 20:24:32 2005 GMT
    Serial Number: 3F619B7E000000000042
        Revocation Date: Sep  8 21:40:48 2005 GMT
    Serial Number: 6313C463000000000052
        Revocation Date: Sep 19 17:37:18 2005 GMT
    Serial Number: 7C3861E3000000000060
        Revocation Date: Sep 20 17:52:56 2005 GMT
    Serial Number: 7C6EE351000000000061
```

```
        Revocation Date: Sep 20 18:52:30 2005 GMT
    Serial Number: 0A338EA1000000000074   <-- Revoked identity certificate
        Revocation Date: Nov 12 04:34:42 2005 GMT
    Signature Algorithm: sha1WithRSAEncryption
        0b:cb:dd:43:0a:b8:62:1e:80:95:06:6f:4d:ab:0c:d8:8e:32:
        44:8e:a7:94:97:af:02:b9:a6:9c:14:fd:eb:90:cf:18:c9:96:
        29:bb:57:37:d9:1f:d5:bd:4e:9a:4b:18:2b:00:2f:d2:6e:c1:
        1a:9f:1a:49:b7:9c:58:24:d7:72
```

Note The identity certificate for the device that was revoked (serial number 0A338EA1000000000074) is listed at the end.

Additional References for PKI

This section includes additional information related to implementing PKI.

Related Documents for PKI

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
VRF configuration	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*

Standards for PKI

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

CHAPTER 10

Configuring User Accounts and RBAC

This chapter describes how to configure user accounts and role-based access control (RBAC) on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About User Accounts and RBAC

You can create and manage users accounts and assign roles that limit access to operations on the Cisco NX-OS device. RBAC allows you to define the rules for an assign role that restrict the authorization that the user has to access management operations.

User Accounts

You can configure up to a maximum of 256 user accounts. By default, the user account does not expire unless you explicitly configure it to expire. The expire option determines the date when the user account is disabled.

Users can have user accounts on multiple VDCs. These users can move between VDCs after an initial connection to a VDC.

The following words are reserved and cannot be used to configure users: bin, daemon, adm, lp, sync, shutdown, halt, mail, news, uucp, operator, games, gopher, ftp, nobody, nscd, mailnull, root, rpc, rpcuser, xfs, gdm, mtsuser, ftpuser, man, and sys.

Note User passwords are not displayed in the configuration files.

Caution Usernames must begin with an alphanumeric character in Cisco NX-OS Releases 6.x and earlier releases. Usernames can contain only these special characters: (+ = . _ \ -). The # and ! symbols are not supported. If the username contains characters that are not allowed, the specified user is unable to log in.

Note Usernames that begin with special characters (+ = . _ \ -) are not supported in Cisco NX-OS Releases 6.x and earlier releases.

Characteristics of Strong Passwords

A strong password has the following characteristics:

- Is at least eight characters long
- Does not contain many consecutive characters (such as abcd)
- Does not contain many repeating characters (such as aaabbb)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

The following are examples of strong passwords:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Note All printable ASCII characters are supported in the password string if they are enclosed in quotation marks.

Note Beginning with Cisco NX-OS Release 7.1, the PSB 5.0 requirements in NXOS are supported.
SEC-PWD-DEFMIN - Default minimum passphrase length must be non-zero and at least eight characters.
The user interface may use the word PASSPHRASES as pass phrases or passphrases rather than as password.

If a password is trivial (such as a short, easy-to-decipher password), the Cisco NX-OS software will reject your password configuration if password-strength checking is enabled. Be sure to configure a strong password as shown in the sample configuration. Passwords are case sensitive.

Related Topics

Enabling Password-Strength Checking, on page 242

User Roles

User roles contain rules that define the operations allowed for the user who is assigned the role. Each user role can contain multiple rules and each user can have multiple roles. For example, if role1 allows access only to configuration operations, and role2 allows access only to debug operations, then users who belong to both role1 and role2 can access configuration and debug operations. You can also limit access to specific VLANs, virtual routing and forwarding instances (VRFs), and interfaces.

The Cisco NX-OS software provides four default user roles:

- network-admin—Complete read-and-write access to the entire Cisco NX-OS device (only available in the default VDC)
- attribute-admin—Complete read-and-write access to the entire Cisco NX-OS device (only available in the default VDC)
- network-operator—Complete read access to the entire Cisco NX-OS device (only available in the default VDC)
- vdc-admin—Read-and-write access limited to a VDC
- vdc-operator—Read access limited to a VDC

Note You cannot change the default user roles.

Note Some **show** commands may be hidden from network-operator and vdc-operator users. In addition, some non-**show** commands (such as **telnet**) may be available for these user roles.

You can create custom roles within a VDC. By default, the user accounts without administrator roles can access only the **show**, **exit**, **end**, and **configure terminal** commands. You can add rules to allow users to configure features.

The VDCs on the same physical device do not share user roles. Each VDC maintains an independent user role database. Within a VDC, roles are configured by rule and attribute assignment.

Note If you belong to multiple roles, you can execute a combination of all the commands permitted by these roles. Access to a command takes priority over being denied access to a command. For example, suppose a user has RoleA, which denied access to the configuration commands. However, the user also has RoleB, which has access to the configuration commands. In this case, the user has access to the configuration commands.

Note Only network-admin user can perform a Checkpoint or Rollback in the RBAC roles. Though other users have these commands as a permit rule in their role, the user access is denied when you try to execute these commands.

User Role Rules

The rule is the basic element of a role. A rule defines what operations the role allows the user to perform. You can apply rules for the following parameters:

Command
: A command or group of commands defined in a regular expression.

Feature
: A command or group of commands defined in a regular expression.

Feature group
: Default or user-defined group of features.

OID
: An SNMP object identifier (OID).

The command, feature, and feature group parameters create a hierarchical relationship. The most basic control parameter is the command. The next control parameter is the feature, which represents all commands associated with the feature. The last control parameter is the feature group. The feature group combines related features and allows you to easily manage the rules. The Cisco NX-OS software also supports the predefined feature group L3 that you can use.

You can configure up to 256 rules for each role. The user-specified rule number determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

User Role Configuration Distribution

Cisco Fabric Services (CFS) allows the Cisco NX-OS device to distribute the user role configuration to other Cisco NX-OS devices in the network. When you enable CFS distribution for a feature on your device, the device belongs to a CFS region containing other devices in the network that you have also enabled for CFS distribution for the feature. CFS distribution for the user role feature is disabled by default.

Note You must explicitly enable CFS for user roles on each device to which you want to distribute configuration changes.

After you enable CFS distribution for user roles on your Cisco NX-OS device, the first user role configuration command that you enter causes the Cisco NX-OS software to take the following actions:

- Creates a CFS session on your Cisco NX-OS device.
- Locks the user role configuration on all Cisco NX-OS devices in the CFS region with CFS enabled for the user role feature.
- Saves the user role configuration changes in a temporary buffer on the Cisco NX-OS device.

The changes stay in the temporary buffer on the Cisco NX-OS device until you explicitly commit them to be distributed to the devices in the CFS region. When you commit the changes, the Cisco NX-OS software takes the following actions:

- Applies the changes to the running configuration on your Cisco NX-OS device.
- Distributes the updated user role configuration to the other Cisco NX-OS devices in the CFS region.
- Unlocks the user role configuration in the devices in the CFS region.
- Terminates the CFS session.

For detailed information on CFS, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.

Virtualization Support for RBAC

The users with the network-admin and network-operator roles can operate in all virtual device contexts (VDCs) when logged in from the default VDC and use the **switchto vdc** command to access other VDCs. All other user roles are local to the VDC. Roles are not shared between VDCs. Each VDC maintains an independent user role database.

The following guidelines and limitations apply to the **switchto vdc** command:

- Only users with the network-admin or network-operator role can use the **switchto vdc** command. No other users are permitted to use it.
- No user can grant permission to another role to use the **switchto vdc** command.
- After a network-admin uses the **switchto vdc** command, this user becomes a vdc-admin for the new VDC. Similarly, after a network-operator uses the **switchto vdc** command, this user becomes a vdc-operator for the new VDC. Any other roles associated with the user are not valid after the **switchto vdc** command is entered.
- After a network-admin or network-operator uses the switchto vdc command, this user cannot use this command to switch to another VDC. The only option is to use the **switchback** command to return to the original VDC.

Beginning with Cisco NX-OS Release 5.2, you can configure RBAC in the storage VDC. Note that RBAC in the storage VDC is RBAC for the Cisco Nexus 7000 Series switches, which is different from that for the Cisco MDS 9500 Series switches.

Note For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Guidelines and Limitations for User Accounts and RBAC

User accounts and RBAC have the following configuration guidelines and limitations:

- You can create up to 64 user-defined roles in a VDC in addition to the four default user roles in the default VDC and the two default user roles in the nondefault VDCs.
- You can add up to 256 rules to a user role.
- You can add up to 64 user-defined feature groups to a VDC in addition to the default feature group, L3.
- You can configure up to 256 users in a VDC.
- You can assign a maximum of 64 user roles to a user account.
- If you have a user account configured on the local Cisco NX-OS device that has the same name as a remote user account on an AAA server, the Cisco NX-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.
- You cannot delete the default admin and SNMP user accounts.
- You cannot remove the default user roles from the default admin user accounts.
- The network-operator and vdc-operator roles cannot run the **show running-config** and **show startup-config** commands.
- RBAC is not supported for traffic between F1 Series module ports and M1 Series module ports in the same VLAN.
- When you have the attribute-admin privilege, you can have multiple roles along with the network-admin capability.
- When you create attribute-admin and an unsupported image is present in the fabric, the role distribute does not fail. The role distribute gets accepted but displays an invalid rule for the unsupported rule.
- The role distribute does not fail for mutually exclusive configurationss if an unsupported image is present in the fabric.
- Loading dplug-image or the show tech command might not work for the custom-role attribute in Cisco NX-OS Release 8.x.
- Downgrading to a Cisco release/image without the attribute-admin is not supported. You need to check about the attribute-admin in an image using the **show role** command.
- Beginning with Cisco NX-OS Release 6.0, RBAC is supported for F2 Series modules.
- The following guidelines are applicable for the **rule** command:
    - When you use the **rule** *rule-id* **permit command** *command-string* command, the *command-string* argument should be complete or it should contain an asterisk (*) after the command name, for example, **show *** or **show running-config ***.

- If you are adding more than one command in the command-string argument, the commands should be separated by a command separator (;) and a whitespace should be added.
- When you are specifying interfaces, it is recommended to specify the entire media type keyword such as Ethernet or loopback. However, if you are using the short form of the media type keyword, it should be followed by an asterisk (*).

  For example, **rule 22 permit command show run int Ethernet4/1**, **rule 22 permit command show run int loopback1**, or **rule 22 permit command show run int eth***.

  Rules that do not follow this guideline are not accepted. For example, **rule 22 permit command show run int Eth1/4** and **rule 22 permit command show run int loop1**. For more information about using the **rule** command, see Creating User Roles and Rules, on page 245.

Note 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 User Accounts and RBAC

This table lists the default settings for user accounts and RBAC parameters.

Table 18: Default User Accounts and RBAC Parameters

Parameters	Default
User account password	Undefined.
User account expiry date	None.
User account role in the default VDC	Network-operator if the creating user has the network-admin role, or vdc-operator if the creating user has the vdc-admin role.
User account role in the non-VDCs	Vdc-operator if the creating user has the vdc-admin role.
Default user roles in the default VDC	Network-operator.
Default user roles in the non-default VDCs	Vdc-operator.
Interface policy	All interfaces are accessible.
VLAN policy	All VLANs are accessible.
VRF policy	All VRFs are accessible.
Feature group	L3.

Enabling Password-Strength Checking

You can enable password-strength checking which prevents you from creating weak passwords for user accounts.

Note When you enable password-strength checking, the Cisco NX-OS software does not check the strength of existing passwords.

SUMMARY STEPS

1. **configure terminal**
2. **password strength-check**
3. **exit**
4. (Optional) **show password strength-check**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**password strength-check** **Example:** `switch(config)# password strength-check`	Enables password-strength checking. The default is enabled. You can disable password-strength checking by using the **no** form of this command.

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

Step 4	(Optional) **show password strength-check** **Example:** `switch# show password strength-check`	Displays the password-strength check configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Characteristics of Strong Passwords, on page 236

Configuring User Accounts

You can create a maximum of 256 user accounts on a Cisco NX-OS device. User accounts have the following attributes:

- Username
- Password
- Expiry date
- User roles

You can enter the password in clear text format or encrypted format. The Cisco NX-OS password encrypts clear text passwords before saving them to the running configuration. Encrypted format passwords are saved to the running configuration without further encryption. MD5 is the default hashing algorithm used for password encryption. As a part of the encryption, a 5000 iteration of 64-bit SALT is added to the password.

User accounts can have a maximum of 64 user roles. The user can determine what commands are available by using the command-line interface (CLI) context sensitive help utility.

Note Changes to user account attributes do not take effect until the user logs in and creates a new session.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **show role**
3. **username** *user-id* [**password** [**0** | **5**] *password*] [**expire** *date*] [**role** *role-name*]
4. **exit**
5. (Optional) **show user-account**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **show role** **Example:** `switch(config)# show role`	Displays the user roles available. You can configure other user roles, if necessary.
Step 3	**username** *user-id* [**password** [**0** | **5**] *password*] [**expire** *date*] [**role** *role-name*] **Example:**	Configures a user account. The *user-id* argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters. Valid characters are uppercase letters A through Z, lowercase letters a through

	Command or Action	Purpose
	`switch(config)# username NewUser password 4Ty18Rnt`	z, numbers 0 through 9, hypen (-), period (.), underscore (_), plus sign (+), and equal sign (=). The at symbol (@) is supported in remote usernames but not in local usernames. The default password is undefined. The **0** option indicates that the password is clear text, and the **5** option indicates that the password is encrypted. The default is **0** (clear text). After creating a user you can associate the user account with the configured custom role. **Note** If you do not specify a password, the user might not be able to log in to the Cisco NX-OS device. **Note** If you create a user account with the encrypted password option, the corresponding SNMP user will not be created. **Note** You do not get the online help option after you specify a password. The help option is provided after the password is entered. The **expire** *date* option format is YYYY-MM-DD. The default is no expiry date. User accounts can have a maximum of 64 user roles.

Step 4	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 5	(Optional) **show user-account** **Example:** `switch# show user-account`	Displays the role configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring Roles, on page 244
Creating User Roles and Rules, on page 245

Configuring Roles

This section describes how to configure user roles.

Enabling User Role Configuration Distribution

To distribute the user roles configuration to other Cisco NX-OS devices in the network, you must first enable CFS distribution for user roles.

SUMMARY STEPS

1. **configure terminal**
2. **role distribute**
3. **exit**
4. (Optional) **show role session status**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**role distribute** **Example:** `switch(config)# role distribute`	Enables user role configuration distribution. The default is disabled.

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

Step 4	(Optional) **show role session status** **Example:** `switch# show role session status`	Displays the user role distribution status information.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Creating User Roles and Rules

You can configure up to 64 user roles in a VDC. Each user role can have up to 256 rules. You can assign a user role to more than one user account.

The rule number that you specify determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

Note Regardless of the read-write rule configured for a user role, some commands can be executed only through the predefined network-admin and vdc-admin roles. For more information on user roles, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Note Whenever a user role or privilege of a user account is changed, the changed role shall come into effect for subsequent logins only.

Before you begin

If you want to distribute the user role configuration, enable user role configuration distribution on all Cisco NX-OS devices to which you want the configuration distributed.

SUMMARY STEPS

1. **configure terminal**
2. **role name** *role-name*
3. **rule** *number* **attribute-admin**
4. **rule** *number* {**deny** | **permit**} **command** *command-string*
5. **rule** *number* {**deny** | **permit**} {**read** | **read-write**}
6. **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*
7. **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name*
8. **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **oid** *snmp_oid_name*
9. (Optional) **description** *text*
10. **exit**
11. (Optional) **show role**
12. (Optional) **show role** {**pending** | **pending-diff**}
13. (Optional) **role commit**
14. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**role name** *role-name*
	
	Example:
	`switch(config)# role name UserA`
	`switch(config-role)#`
		Specifies a user role and enters role configuration mode. The *role-name* argument is a case-sensitive, alphanumeric character string with a maximum length of 16 characters.

	Command or Action	Purpose
Step 3	**rule** *number* **attribute-admin** **Example:** `switch(config-role)# rule 1 attribute-admin`	Configures a command rule with a custom role with full network-admin capability so that you can modify other user's role or password administration. The attribute-admin rule is mutually exclusive with the other rules.
Step 4	**rule** *number* {**deny** | **permit**} **command** *command-string* **Example:** `switch(config-role)# rule 1 deny command clear users`	Configures a command rule. The *command-string* argument can contain spaces and regular expressions. For example, interface ethernet includes all Ethernet interfaces. Repeat this command for as many rules as needed. For more information about guidelines for this command, see Guidelines and Limitations for User Accounts and RBAC, on page 240.
Step 5	**rule** *number* {**deny** | **permit**} {**read** | **read-write**} **Example:** `switch(config-role)# rule 2 deny read-write`	Configures a read-only or read-and-write rule for all operations.
Step 6	**rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name* **Example:** `switch(config-role)# rule 3 permit read feature router-bgp`	Configures a read-only or read-and-write rule for a feature. Use the **show role feature** command to display a list of features. Repeat this command for as many rules as needed.
Step 7	**rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name* **Example:** `switch(config-role)# rule 4 deny read-write feature-group L3`	Configures a read-only or read-and-write rule for a feature group. Use the **show role feature-group** command to display a list of feature groups. Repeat this command for as many rules as needed.
Step 8	**rule** *number* {**deny** | **permit**} {**read** | **read-write**} **oid** *snmp_oid_name* **Example:** `switch(config-role)# rule 5 deny read-write oid 1.3.6.1.2.1.1.9`	Configures a read-only or read-and-write rule for an SNMP object identifier (OID). You can enter up to 32 elements for the OID. This command can be used to allow SNMP-based performance monitoring tools to poll devices but restrict their access to system-intensive branches such as the IP routing table, ARP cache, MAC address tables, specific MIBs, and so on. **Note** The deepest OID can be at the scalar level or at the table root level. Repeat this command for as many rules as needed.
Step 9	(Optional) **description** *text* **Example:** `switch(config-role)# description This role does not allow users to use clear commands`	Configures the role description. You can include spaces in the description.

	Command or Action	Purpose

Step 10	**exit**
	Example:
	`switch(config-role)# exit`
	`switch(config)#`
		Exits role configuration mode.

Step 11	(Optional) **show role** **Example:** `switch(config)# show role`	Displays the user role configuration.
Step 12	(Optional) **show role** {**pending** | **pending-diff**} **Example:** `switch(config)# show role pending`	Displays the user role configuration pending for distribution.
Step 13	(Optional) **role commit** **Example:** `switch(config)# role commit`	Applies the user role configuration changes in the temporary database to the running configuration and distributes user role configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.
Step 14	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Committing the User Role Configuration to Distribution, on page 254

Creating Feature Groups

You can create custom feature groups to add to the default list of features provided by the Cisco NX-OS software. These groups contain one or more of the features. You can create up to 64 feature groups in a VDC.

Note You cannot change the default feature group L3.

Before you begin

If you want to distribute the user role configuration, enable user role configuration distribution on all Cisco NX-OS devices to which you want the configuration distributed.

SUMMARY STEPS

1. **configure terminal**
2. **role feature-group name** *group-name*
3. **feature** *feature-name*
4. **exit**

5. (Optional) **show role feature-group**
6. (Optional) **show role** {**pending** | **pending-diff**}
7. (Optional) **role commit**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**role feature-group name** *group-name*
	Example:
	`switch(config)# role feature-group name GroupA`
	`switch(config-role-featuregrp)#`
		Specifies a user role feature group and enters role feature group configuration mode.
		The *group-name* argument is a case-sensitive, alphanumeric character string with a maximum length of 32 characters.

Step 3	**feature** *feature-name* **Example:** `switch(config-role-featuregrp)# feature vdc`	Specifies a feature for the feature group. Repeat this command for as many features as needed. **Note** Use the **show role component** command to display a list of features.

Step 4	**exit**
	Example:
	`switch(config-role-featuregrp)# exit`
	`switch(config)#`
		Exits role feature group configuration mode.

Step 5	(Optional) **show role feature-group** **Example:** `switch(config)# show role feature-group`	Displays the role feature group configuration.
Step 6	(Optional) **show role** {**pending** | **pending-diff**} **Example:** `switch(config)# show role pending`	Displays the user role configuration pending for distribution.
Step 7	(Optional) **role commit** **Example:** `switch(config)# role commit`	Applies the user role configuration changes in the temporary database to the running configuration and distributes user role configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Committing the User Role Configuration to Distribution, on page 254

Changing User Role Interface Policies

You can change a user role interface policy to limit the interfaces that the user can access. By default, a user role allows access to all interfaces in the VDC.

Before you begin

Create one or more user roles.

If you want to distribute the user role configuration, enable user role configuration distribution on all Cisco NX-OS devices to which you want the configuration distributed.

SUMMARY STEPS

1. **configure terminal**
2. **role name** *role-name*
3. **interface policy deny**
4. **permit interface** *interface-list*
5. **exit**
6. (Optional) **show role**
7. (Optional) **show role** {**pending** | **pending-diff**}
8. (Optional) **role commit**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**role name** *role-name*
	
	Example:
	`switch(config)# role name UserA`
	`switch(config-role)#`
		Specifies a user role and enters role configuration mode.

Step 3	**interface policy deny**
	
	Example:
	`switch(config-role)# interface policy deny`
	`switch(config-role-interface)#`
		Enters role interface policy configuration mode.

Step 4	**permit interface** *interface-list* **Example:** `switch(config-role-interface)# permit interface ethernet 2/1-4`	Specifies a list of interfaces that the role can access. Repeat this command for as many interfaces as needed.

	Command or Action	Purpose

Step 5	**exit**
	Example:
	`switch(config-role-interface)# exit`
	`switch(config-role)#`
		Exits role interface policy configuration mode.

Step 6	(Optional) **show role** **Example:** `switch(config-role)# show role`	Displays the role configuration.
Step 7	(Optional) **show role** {**pending** | **pending-diff**} **Example:** `switch(config-role)# show role pending`	Displays the user role configuration pending for distribution.
Step 8	(Optional) **role commit** **Example:** `switch(config-role)# role commit`	Applies the user role configuration changes in the temporary database to the running configuration and distributes user role configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config-role)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Creating User Roles and Rules, on page 245
Committing the User Role Configuration to Distribution, on page 254

Changing User Role VLAN Policies

You can change a user role VLAN policy to limit the VLANs that the user can access. By default, a user role allows access to all VLANs in the VDC.

Before you begin

Create one or more user roles.

If you want to distribute the user role configuration, enable user role configuration distribution on all Cisco NX-OS devices to which you want the configuration distributed.

SUMMARY STEPS

1. **configure terminal**
2. **role name** *role-name*
3. **vlan policy deny**
4. **permit vlan** *vlan-list*
5. **exit**

6. (Optional) **show role**
7. (Optional) **show role** {**pending** | **pending-diff**}
8. (Optional) **role commit**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**role name** *role-name*
	Example:
	`switch(config)# role name UserA`
	`switch(config-role)#`
		Specifies a user role and enters role configuration mode.

Step 3	**vlan policy deny**
	Example:
	`switch(config-role)# vlan policy deny`
	`switch(config-role-vlan)#`
		Enters role VLAN policy configuration mode.

Step 4	**permit vlan** *vlan-list* **Example:** `switch(config-role-vlan)# permit vlan 1-4`	Specifies a range of VLANs that the role can access. Repeat this command for as many VLANs as needed.

Step 5	**exit**
	Example:
	`switch(config-role-vlan)# exit`
	`switch(config-role)#`
		Exits role VLAN policy configuration mode.

Step 6	(Optional) **show role** **Example:** `switch(config)# show role`	Displays the role configuration.
Step 7	(Optional) **show role** {**pending** | **pending-diff**} **Example:** `switch(config-role)# show role pending`	Displays the user role configuration pending for distribution.
Step 8	(Optional) **role commit** **Example:** `switch(config-role)# role commit`	Applies the user role configuration changes in the temporary database to the running configuration and distributes user role configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.
Step 9	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	`switch(config-role)# copy running-config startup-config`	

Related Topics

Creating User Roles and Rules, on page 245
Committing the User Role Configuration to Distribution, on page 254

Changing User Role VRF Policies

You can change a user role VRF policy to limit the VRFs that the user can access. By default, a user role allows access to all VRFs in the VDC.

Before you begin

Create one or more user roles.

If you want to distribute the user role configuration, enable user role configuration distribution on all Cisco NX-OS devices to which you want the configuration distributed.

SUMMARY STEPS

1. **configure terminal**
2. **role name** *role-name*
3. **vrf policy deny**
4. **permit vrf** *vrf-name*
5. **exit**
6. (Optional) **show role**
7. (Optional) **show role** {**pending** | **pending-diff**}
8. (Optional) **role commit**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**role name** *role-name*
	Example:
	`switch(config)# role name UserA`
	`switch(config-role)#`
		Specifies a user role and enters role configuration mode.

Step 3	**vrf policy deny** **Example:**	Enters role VRF policy configuration mode.

	Command or Action	Purpose
	`switch(config-role)# vrf policy deny` `switch(config-role-vrf)#`	
Step 4	**permit vrf** *vrf-name* **Example:** `switch(config-role-vrf)# permit vrf vrf1`	Specifies the VRF that the role can access. Repeat this command for as many VRFs as needed.

Step 5	**exit**
	Example:
	`switch(config-role-vrf)# exit`
	`switch(config-role)#`
		Exits role VRF policy configuration mode.

Step 6	(Optional) **show role** **Example:** `switch(config-role)# show role`	Displays the role configuration.
Step 7	(Optional) **show role** {**pending** | **pending-diff**} **Example:** `switch(config-role)# show role pending`	Displays the user role configuration pending for distribution.
Step 8	(Optional) **role commit** **Example:** `switch(config-role)# role commit`	Applies the user role configuration changes in the temporary database to the running configuration and distributes user role configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config-role)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Creating User Roles and Rules, on page 245
Committing the User Role Configuration to Distribution, on page 254

Committing the User Role Configuration to Distribution

You can apply the user role global and/or server configuration stored in the temporary buffer to the running configuration across all switches in the fabric (including the originating switch).

Before you begin

You have enabled user role configuration distribution on the Cisco NX-OS device.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **show role** {**pending** | **pending-diff**}

3. (Optional) **role commit**
4. **exit**
5. (Optional) **show role session status**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **show role** {**pending** | **pending-diff**} **Example:** `switch(config)# show role pending`	Displays the user role configuration pending for distribution.
Step 3	(Optional) **role commit** **Example:** `switch(config)# role commit`	Applies the user role configuration changes in the temporary database to the running configuration and distributes user role configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show role session status** **Example:** `switch# show role session status`	Displays the user role CFS session status.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Applies the running configuration to the startup configuration on all Cisco NX-OS devices in the network that have CFS enabled.

Related Topics

User Role Configuration Distribution, on page 238

Discarding the User Role Distribution Session

You can discard the temporary database of user role changes and end the CFS distribution session.

Before you begin

You have enabled user role configuration distribution on the Cisco NX-OS device.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **show role** {**pending** | **pending-diff**}
3. **role abort**
4. **exit**
5. (Optional) **show role session status**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **show role** {**pending** | **pending-diff**} **Example:** `switch(config)# show role pending`	Displays the user role configuration pending for distribution.
Step 3	**role abort** **Example:** `switch(config)# role abort`	Discards the user role configuration in the temporary storage and ends the session.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show role session status** **Example:** `switch# show role session status`	Displays the user role CFS session status.

Related Topics

Committing the User Role Configuration to Distribution, on page 254
User Role Configuration Distribution, on page 238

Clearing the User Role Distribution Session

You can clear the ongoing Cisco Fabric Services distribution session (if any) and unlock the fabric for the user role feature.

You have enabled user role configuration distribution on the Cisco NX-OS device.

SUMMARY STEPS

1. **clear role session**
2. (Optional) **show role session status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clear role session** **Example:** `switch# clear role session`	Clears the session and unlocks the fabric.
Step 2	(Optional) **show role session status** **Example:** `switch# show role session status`	Displays the user role CFS session status.

Related Topics

Committing the User Role Configuration to Distribution, on page 254
User Role Configuration Distribution, on page 238

Verifying User Accounts and RBAC Configuration

To display user account and RBAC configuration information, perform one of the following tasks:

Command	Purpose
show cli syntax roles network-admin	Displays the syntax of the commands that the network-admin role can use but the vdc-admin role cannot.
show cli syntax roles network-operator	Displays the syntax of the commands that the network-operator role can use but the vdc-operator role cannot.
show role	Displays the user role configuration.
show role feature	Displays the feature list.
show role feature-group	Displays the feature group configuration.
show startup-config security	Displays the user account configuration in the startup configuration.
show running-config security [**all**]	Displays the user account configuration in the running configuration. The **all** keyword displays the default values for the user accounts.
show user-account	Displays user account information.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuration Examples for User Accounts and RBAC

The following example shows how to configure a user role:

```
role name User-role-A
  rule 3 permit read-write feature l2nac
  rule 2 permit read-write feature dot1x
  rule 1 deny command clear *
```

The following example shows how to create a user role that can configure an interface to enable and show HSRP and show GLBP:

```
role name iftest
   rule 1 permit command config t; interface *; hsrp *
   rule 2 permit read-write feature hsrp
   rule 3 permit read feature glbp
```

In the above example, rule 1 allows you to configure HSRP on an interface, rule 2 allows you to configure the **config hsrp** commands and enable the exec-level **show** and **debug** commands for HSRP, and rule 3 allows you to enable the exec-level **show** and **debug glbp** commands.

The following example shows how to configure a user role that can configure only a specific interface:

```
role name Int_Eth2-3_only
  rule 1 permit command configure terminal; interface *
  interface policy deny
    permit interface Ethernet2/3
```

The following example shows how to configure a user role feature group:

```
role feature-group name Security-features
  feature radius
  feature tacacs
  feature dot1x
  feature aaa
  feature l2nac
  feature acl
  feature access-list
```

The following example shows how to configure a user account:

```
username user1 password A1s2D4f5 role User-role-A
```

The following example shows the display of the help option after you specify a password:

```
switch(config)# username user1 password?
  password  Password for the user (no help for the next token, please refer the

            config guide for usage)

switch(config)# username user1 password 0?!2ad ?
```

```
  <CR>
  expire    Expiry date for this user account(in YYYY-MM-DD format)
  priv-lvl  Privilege level which the user is to be assigned to
  role      Role which the user is to be assigned to
```

The following example shows how to add an OID rule to restrict access to part of the OID subtree:

```
role name User1
  rule 1 permit read feature snmp
  rule 2 deny read oid 1.3.6.1.2.1.1.9
show role name User1

Role: User1
  Description: new role
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  -------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  -------------------------------------------------------------------
  2       deny    read        oid                 1.3.6.1.2.1.1.9
  1       permit  read        feature             snmp
```

The following example shows how to give write permission to a specified OID subtree:

```
role name User1
rule 3 permit read-write oid 1.3.6.1.2.1.1.5
show role name User1

Role: User1
  Description: new role
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  -------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  -------------------------------------------------------------------
  3       permit  read-write  oid                 1.3.6.1.2.1.1.5
  2       deny    read        oid                 1.3.6.1.2.1.1.9
  1       permit  read        feature             snmp
```

Additional References for User Accounts and RBAC

This section includes additional information related to implementing user accounts and RBAC.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
VRF configuration	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

- CISCO-COMMON-MGMT-MIB

Related Documents for User Accounts and RBAC

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
VRF configuration	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*

Standards for User Accounts and RBAC

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs for User Accounts and RBAC

MIBs	MIBs Link
• CISCO-COMMON-MGMT-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for User Accounts and RBAC

This table lists the release history for this feature.

Table 19: Feature History for User Accounts and RBAC

Feature Name	Releases	Feature Information
RBAC	6.0(1)	Added support for F2 Series modules.

Feature Name	Releases	Feature Information
User accounts and RBAC	6.0(1)	Added the ability to configure a read-only or read-and-write rule for an SNMP OID.
User accounts and RBAC	5.2(1)	No change from Release 5.1.
User accounts and RBAC	5.2(1)	Added support for the Cisco Nexus 3000 Series Switches.
User roles	5.1(1)	Added the ability to display the syntax of the commands that the network-admin and network-operator roles can use.
User accounts and RBAC	5.1(1)	No change from Release 5.0.
User accounts and RBAC	5.0(2)	Added the ability to support the at symbol (@) in remote usernames.
User accounts and RBAC	5.0(2)	No change from Release 4.2.
Usernames	4.2(1)	Valid characters in username are limited to lowercase a through z, uppercase A through Z, the numbers 0 through 9, plus sign (+), hyphen (-), equal sigh (=), underscore (_) and period (.).

CHAPTER 11

Configuring 802.1X

This chapter describes how to configure IEEE 802.1X port-based authentication on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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.

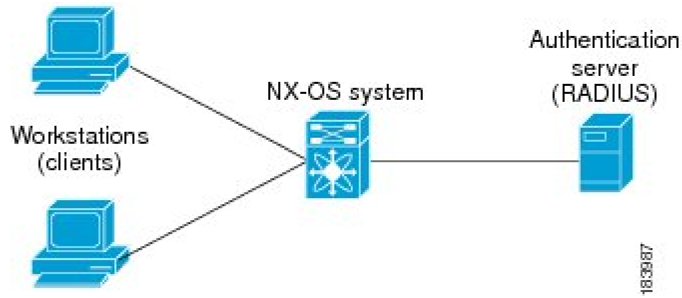
Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

Device Roles

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

Figure 5: 802.1X Device Roles

This figure shows the device roles in 802.1X.



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.

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.

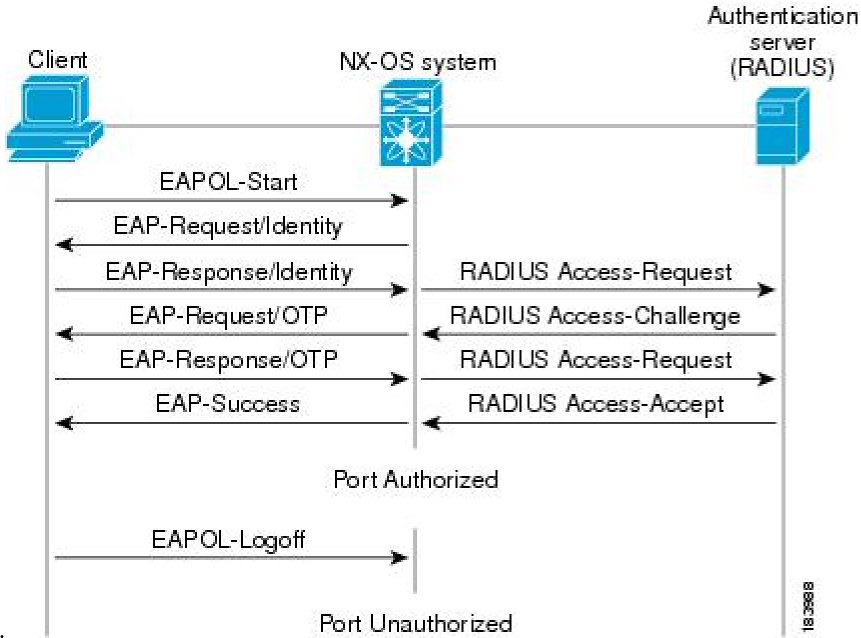
Note If 802.1X is not enabled or supported on the network access device, the Cisco NX-OS device drops any EAPOL frames from the supplicant. If the supplicant does not receive an EAP-request/identity frame after three attempts to start authentication, the supplicant transmits data as if the port is in 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 6: 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.

Related Topics

Ports in Authorized and Unauthorized States, on page 266

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.

Related Topics

802.1X and Port Security, on page 268

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 addressees 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.

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 put 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

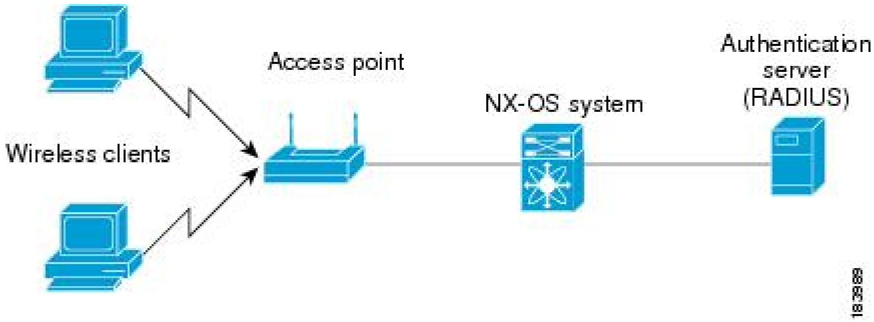
The 802.1X port-based authentication is supported in two topologies:

- 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.

Figure 7: Wireless LAN Example

This figure shows 802.1X port-based authentication in a wireless LAN. The 802.1X port is configured as a multiple-host port that becomes authorized as soon as one supplicant is authenticated.



When the port is authorized, all other hosts indirectly attached to the port are granted access to the network. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), the Cisco NX-OS device denies access to the network to all of the attached supplicants.

Virtualization Support for 802.1X

The 802.1X configuration and operation are local to the virtual device context (VDC). For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Licensing Requirements for 802.1X

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	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. For an explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Prerequisites for 802.1X

802.1X has the following prerequisites:

- One or more RADIUS servers are accessible in the network.
- 802.1X supplicants are attached to the ports, unless you enable MAC address authentication bypass.

Related Topics

Enabling MAC Authentication Bypass, on page 284

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.
- The Cisco NX-OS software supports 802.1X authentication on member ports of a port channel but not on the port channel itself.
- The Cisco NX-OS software does not support the following 802.1X configurations on port channel members when the members are configured for 802.1X:
    - Host mode cannot be configured in single-host mode. Only multi-host mode is supported on the member ports.
    - MAC authentication bypass cannot be enabled on the member ports.
    - Port security cannot be configured on the port channel.
- Member ports with and without 802.1X configuration can coexist in a port channel. However, you must ensure the identical 802.1X configuration on all the member ports in order for channeling to operate with 802.1X.
- 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
- The Cisco NX-OS software does not support dynamic VLAN assignment on the Cisco Nexus 7000 series switches.

Default Settings for 802.1X

This table lists the default settings for 802.1X parameters.

Table 20: Default 802.1X Parameters

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

Configuring 802.1X

This section describes how to configure the 802.1X feature.

Note 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.

Process for Configuring 802.1X

This section describes the process for configuring 802.1X.

SUMMARY STEPS

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

DETAILED STEPS

Step 1 Enable the 802.1X feature.

Step 2 Configure the connection to the remote RADIUS server.

Step 3 Enable 802.1X feature on the Ethernet interfaces.

Related Topics

Enabling the 802.1X Feature, on page 273
Configuring AAA Authentication Methods for 802.1X, on page 274
Controlling 802.1X Authentication on an Interface, on page 275

Enabling the 802.1X Feature

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

SUMMARY STEPS

1. **configure terminal**
2. **feature dot1x**
3. **exit**
4. (Optional) **show dot1x**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 2	**feature dot1x** **Example:** `switch(config)# feature dot1x`	Enables the 802.1X feature. The default is disabled.

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

Step 4	(Optional) **show dot1x** **Example:** `switch# show dot1x`	Displays the 802.1X feature status.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication dot1x default group** *group-list*
3. **exit**
4. (Optional) **show radius-server**
5. (Optional) **show radius-server group** [*group-name*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 2	**aaa authentication dot1x default group** *group-list* **Example:** `switch(config)# aaa authentication dot1x default group rad2`	Specifies the RADIUS server groups to use for 802.1X authentication. 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 the global pool of RADIUS servers for authentication.

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

Step 4	(Optional) **show radius-server** **Example:** `switch# show radius-server`	Displays the RADIUS server configuration.
Step 5	(Optional) **show radius-server group** [*group-name*] **Example:** `switch# show radius-server group rad2`	Displays the RADIUS server group configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring AAA, on page 25
Configuring RADIUS, on page 61

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot* / *port*
3. **dot1x port-control** {**auto** | **force-authorized** | **forced-unauthorized**}
4. **exit**
5. (Optional) **show dot1x all**
6. (Optional) **show dot1x interface ethernet** *slot* / *port*
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot* / *port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Selects the interface to configure and enters interface configuration mode.

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.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 5	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	Displays all 802.1X feature status and configuration information.
Step 6	(Optional) **show dot1x interface ethernet** *slot* / *port* **Example:** `switch# show dot1x interface ethernet 2/1`	Displays 802.1X feature status and configuration information for an interface.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the 802.1X Feature, on page 273

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.

Note By default, the Cisco NX-OS software creates the authenticator PAE instance on the interface when you enable 802.1X on an interface.

Before you begin

Enable the 802.1X feature.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **show dot1x interface ethernet** *slot*/*port*
3. **interface ethernet** *slot*/*port*
4. [**no**] **dot1x pae authenticator**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **show dot1x interface ethernet** *slot*/*port* **Example:** `switch# show do1x interface ethernet 2/1`	Displays the 802.1X configuration on the interface.

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.

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.

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

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **dot1x re-authentication**
4. (Optional) **dot1x timeout re-authperiod** *seconds*
5. **exit**
6. (Optional) **show dot1x all**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot*/*port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Selects the interface to configure and enters interface configuration mode.

Step 3	**dot1x re-authentication** **Example:** `switch(config-if)# dot1x re-authentication`	Enables periodic reauthentication of the supplicants connected to the interface. By default, periodic authentication is disabled.

	Command or Action	Purpose
Step 4	(Optional) **dot1x timeout re-authperiod** *seconds* **Example:** `switch(config-if)# dot1x timeout re-authperiod 3300`	Sets the number of seconds between reauthentication attempts. The default is 3600 seconds. The range is from 1 to 65535. **Note** This command affects the behavior of the Cisco NX-OS device only if you enable periodic reauthentication on the interface.

Step 5	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits configuration mode.

Step 6	(Optional) **show dot1x all** **Example:** `switch(config)# show dot1x all`	Displays all 802.1X feature status and configuration information.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the 802.1X Feature, on page 273
Manually Reauthenticating Supplicants , on page 279

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.

SUMMARY STEPS

1. **dot1x re-authenticate** [**interface** *slot/port*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dot1x re-authenticate** [**interface** *slot/port*] **Example:**	Reauthenticates the supplicants on the Cisco NX-OS device or on an interface.

	Command or Action	Purpose
	`switch# dot1x re-authenticate interface 2/1`	

Related Topics

Enabling the 802.1X Feature, on page 273
Enabling Periodic Reauthentication for an Interface, on page 278

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.

Note Initializing the authentication clears any existing authentication status before starting the authentication process for the client.

Before you begin

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

SUMMARY STEPS

1. **dot1x initialize** [**interface ethernet** *slot/port*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dot1x initialize** [**interface ethernet** *slot/port*] **Example:** `switch# dot1x initialize interface ethernet 2/1`	Initializes 802.1X authentication on the Cisco NX-OS device or on a specified interface.

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-supplicant 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-supplicant 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.

Note 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.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. (Optional) **dot1x timeout quiet-period** *seconds*
4. (Optional) **dot1x timeout ratelimit-period** *seconds*
5. (Optional) **dot1x timeout server-timeout** *seconds*
6. (Optional) **dot1x timeout supp-timeout** *seconds*
7. (Optional) **dot1x timeout tx-period** *seconds*
8. **exit**
9. (Optional) **show dot1x all**
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		Selects the interface to configure and enters interface configuration mode.

	Command or Action	Purpose
Step 3	(Optional) **dot1x timeout quiet-period** *seconds* **Example:** `switch(config-if)# dot1x timeout quiet-period 25`	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.
Step 4	(Optional) **dot1x timeout ratelimit-period** *seconds* **Example:** `switch(config-if)# dot1x timeout ratelimit-period 10`	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.
Step 5	(Optional) **dot1x timeout server-timeout** *seconds* **Example:** `switch(config-if)# dot1x timeout server-timeout 60`	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.
Step 6	(Optional) **dot1x timeout supp-timeout** *seconds* **Example:** `switch(config-if)# dot1x timeout supp-timeout 20`	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.
Step 7	(Optional) **dot1x timeout tx-period** *seconds* **Example:** `switch(config-if)# dot1x timeout tx-period 40`	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.

Step 8	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 9	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	Displays the 802.1X configuration.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the 802.1X Feature, on page 273

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **dot1x host-mode** {**multi-host** | **single-host**}
4. **exit**
5. (Optional) **show dot1x all**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		Selects the interface to configure and enters interface configuration mode.

Step 3	**dot1x host-mode** {**multi-host** | **single-host**} **Example:** `switch(config-if)# dot1x host-mode multi-host`	Configures the host mode. The default is single-host. **Note** Make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified interface.

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits configuration mode.

Step 5	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	Displays all 802.1X feature status and configuration information.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the 802.1X Feature, on page 273

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **dot1x mac-auth-bypass** [**eap**]
4. **exit**
5. (Optional) **show dot1x all**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot*/*port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		Selects the interface to configure and enters interface configuration mode.

Step 3	**dot1x mac-auth-bypass** [**eap**] **Example:** `switch(config-if)# dot1x mac-auth-bypass`	Enables MAC authentication bypass. The default is bypass disabled. Use the **eap** keyword to configure the Cisco NX-OS device to use EAP for authorization.

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits configuration mode.

Step 5	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	Displays all 802.1X feature status and configuration information.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the 802.1X Feature, on page 273

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.

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.

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **no dot1x system-auth-control**
3. **exit**
4. (Optional) **show dot1x**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no dot1x system-auth-control** **Example:** `switch(config)# no dot1x system-auth-control`	Disables 802.1X authentication on the Cisco NX-OS device. The default is enabled. **Note** Use the **dot1x system-auth-control** command to enable 802.1X authentication on the Cisco NX-OS device.

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

	Command or Action	Purpose
Step 4	(Optional) **show dot1x** **Example:** `switch# show dot1x`	Displays the 802.1X feature status.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the 802.1X Feature, on page 273
Controlling 802.1X Authentication on an Interface, on page 275

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.

SUMMARY STEPS

1. **configure terminal**
2. **no feature dot1x**
3. **exit**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no feature dot1x** **Example:** `switch(config)# no feature dot1x`	Disables 802.1X. **Caution** Disabling the 802.1X feature removes all 802.1X configuration.
Step 3	**exit** **Example:**	Exits configuration mode.

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the 802.1X Feature, on page 273
Disabling 802.1X Authentication on the Cisco NX-OS Device, on page 285

Resetting the 802.1X Interface Configuration to the Default Values

You can reset the 802.1X configuration for an interface to the default values.

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **dot1x default**
4. **exit**
5. (Optional) **show dot1x all**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		Selects the interface to configure and enters interface configuration mode.

Step 3	**dot1x default** **Example:** `switch(config-if)# dot1x default`	Reverts to the 802.1X configuration default values for the interface.

	Command or Action	Purpose

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits configuration mode.

Step 5	(Optional) **show dot1x all** **Example:** `switch(config)# show dot1x all`	Displays all 802.1X feature status and configuration information.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the 802.1X Feature, on page 273

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **dot1x max-req** *count*
4. **exit**
5. (Optional) **show dot1x all**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**interface ethernet** *slot*/*port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Selects the interface to configure and enters interface configuration mode.

Step 3	**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. **Note** Make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified interface.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits interface configuration mode.

Step 5	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	Displays all 802.1X feature status and configuration information.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the 802.1X Feature, on page 273

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.

SUMMARY STEPS

1. **configure terminal**
2. **dot1x radius-accounting**
3. **exit**
4. (Optional) **show dot1x**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**dot1x radius-accounting** **Example:** `switch(config)# dot1x radius-accounting`	Enables RADIUS accounting for 802.1X. The default is disabled.

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

Step 4	(Optional) **show dot1x** **Example:** `switch# show dot1x`	Displays the 802.1X configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the 802.1X Feature, on page 273

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.

SUMMARY STEPS

1. **configure terminal**
2. **aaa accounting dot1x default group** *group-list*
3. **exit**
4. (Optional) **show aaa accounting**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**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.
Step 3	**exit**	Exits configuration mode.
Step 4	(Optional) **show aaa accounting**	Displays the AAA accounting configuration.
Step 5	(Optional) **copy running-config startup-config**	Copies the running configuration to the startup configuration.

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
switch# show aaa accounting
switch# copy running-config startup-config
```

Related Topics

Enabling the 802.1X Feature, on page 273

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **dot1x max-reauth-req** *retry-count*
4. **exit**

5. (Optional) **show dot1x all**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Selects the interface to configure and enters interface configuration mode.

Step 3	**dot1x max-reauth-req** *retry-count* **Example:** `switch(config-if)# dot1x max-reauth-req 3`	Changes the maximum reauthentication request retry count. The default is 2 times and the range is from 1 to 10.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits interface configuration mode.

Step 5	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	Displays all 802.1X feature status and configuration information.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the 802.1X Feature, on page 273

Verifying the 802.1X Configuration

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

Command	Purpose
show dot1x	Displays the 802.1X feature status.
show dot1x all [**details** | **statistics** | **summary**]	Displays all 802.1X feature status and configuration information.

Command	Purpose
show dot1x interface ethernet *slot/port* [**details** | **statistics** | **summary**]	Displays the 802.1X feature status and configuration information for an Ethernet interface.
show running-config dot1x [**all**]	Displays the 802.1X feature configuration in the running configuration.
show startup-config dot1x	Displays the 802.1X feature configuration in the startup configuration.

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.

SUMMARY STEPS

1. **show dot1x** {**all** | **interface ethernet** *slot/port*} **statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show dot1x** {**all** | **interface ethernet** *slot/port*} **statistics** **Example:** `switch# show dot1x all statistics`	Displays the 802.1X statistics.

Related Topics

Enabling the 802.1X Feature, on page 273

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.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
VRF configuration	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*

Standards

Standards	Title
IEEE Std 802.1X- 2004 (Revision of IEEE Std 802.1X-2001)	*802.1X IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control*
RFC 2284	*PPP Extensible Authentication Protocol (EAP)*
RFC 3580	*IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*

MIBs

- IEEE8021-PAE-MIB

Feature History for 802.1X

This table lists the release history for this feature:

Table 21: Feature History for 802.1X

Feature Name	Releases	Feature Information
802.1X	6.0(1)	No change from Release 5.2.
802.1X	5.2(1)	No change from Release 5.1.
802.1X	5.1(1)	No change from Release 5.0.

CHAPTER 12

Configuring NAC

This chapter describes how to configure Network Admission Control (NAC) on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About NAC

NAC allows you to check endpoint devices for security compliancy and vulnerability before these devices are allowed access to the network. This security compliancy check is referred to as *posture validation*. Posture validation allows you to prevent the spread of worms, viruses, and other rogue applications across the network.

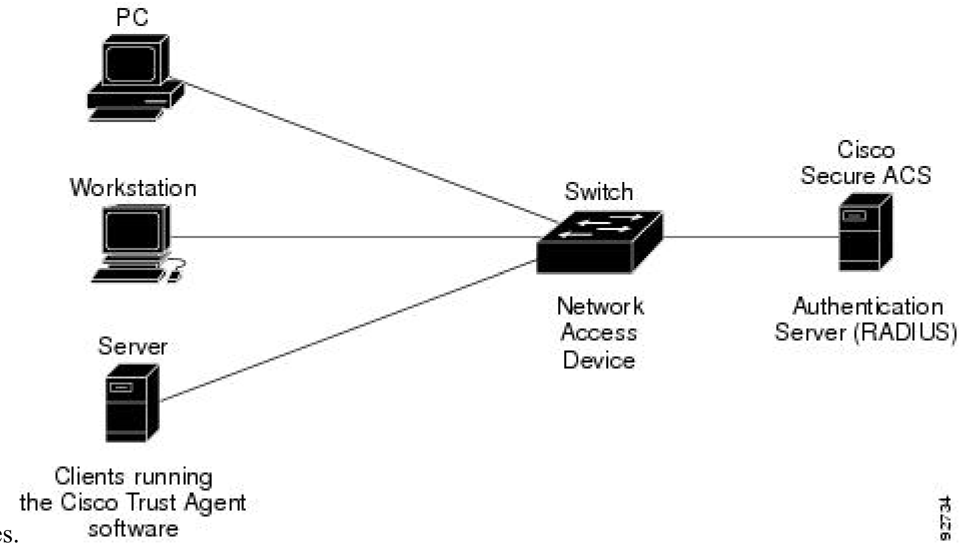
NAC validates that the posture or state of endpoint devices complies with security policies before the devices can access protected areas of the network. For devices that comply with the security policies, NAC allows access to protected services in the network. For devices that do not comply with security policies, NAC allows access to the network only for remediation, when the posture of the device is checked again.

NAC Device Roles

NAC assigns roles to the devices in the network.

Figure 8: Posture Validation Devices

This figure shows an example of a network with the NAC device



roles.

NAC supports the following roles for network devices:

Endpoint device

Systems or clients on the network such as a PC, workstation, or server that is connected to a Cisco NX-OS device access port through a direct connection. The endpoint device, which is running the Cisco Trust Agent software, requests access to the LAN and switch services and responds to requests from the switch. Endpoint devices are potential sources of virus infections, and NAC must validate their antivirus statuses before granting network access.

Note The Cisco Trust Agent software is also referred to as the *posture agent* or the *antivirus client*. For more information on Cisco Trust Agent software, go to the following URL:

http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html

Network access device (NAD)

Cisco NX-OS device that provides validation services and policy enforcement at the network edge and controls the physical access to the network based on the access policy of the client. The NAD relays Extensible Authentication Protocol (EAP) messages between the endpoints and the authentication server.

The NAD queries for posture credentials whenever it detects a new connection to the network. When the endpoint device has a posture agent (PA) installed, the NAD performs an in-band posture validation. The NAD acts as a relay agent between the endpoint device and AAA server for all messages in the posture validation exchange. If the NAD does not find a PA, the NAD performs an out-of-band posture validation through an audit server.

The NAD queries for posture credentials whenever it detects a new connection to the network. When the endpoint device has a posture agent (PA) installed, the NAD performs an in-band posture validation.

The NAD acts as a relay agent between the endpoint device and AAA server for all messages in the posture validation exchange. If the NAD does not find a PA, the NAD performs an out-of-band posture validation through an audit server.

The NAD controls which hosts have access to network destinations through that device based on a network access profile received from the AAA server once the posture validation exchange completes (whether in-band or out-of-band). The access profile can be one of the following forms:

- VLAN or private VLAN.
- Access control lists (ACLs) determine what type of traffic for which destinations are reachable for this host in addition to any default access that is provided to all hosts independent of the NAC process (for example, access to the Dynamic Host Configuration Protocol [DHCP] server, remediation server, audit server).

The NAD triggers the posture validation process at the following times:

- When a new session starts.
- When the revalidation timer expires.
- When you enter a system administrator command.
- When the posture agent indicates that the posture has changed (only for an endpoint device with a posture agent).

For Cisco NX-OS devices, the encapsulation information in the Extensible Authentication Protocol (EAP) messages is based on the User Datagram Protocol (UDP). When using UDP, the Cisco NX-OS device uses EAP over UDP (EAPoUDP or EoU) frames.

Authentication server

Server that performs the actual validation of the client. The authentication server validates the antivirus status of the client, determines the access policy, and notifies the NAD if the client is authorized to access the LAN and NAD services. Because the NAD acts as the proxy, the EAP message exchange between the NAD and authentication server is transparent to the NAD.

The Cisco NX-OS device supports the Cisco Secure Access Control Server (ACS) Version 4.0 or later with RADIUS, authentication, authorization, and accounting (AAA), and EAP extensions.

Posture validation server

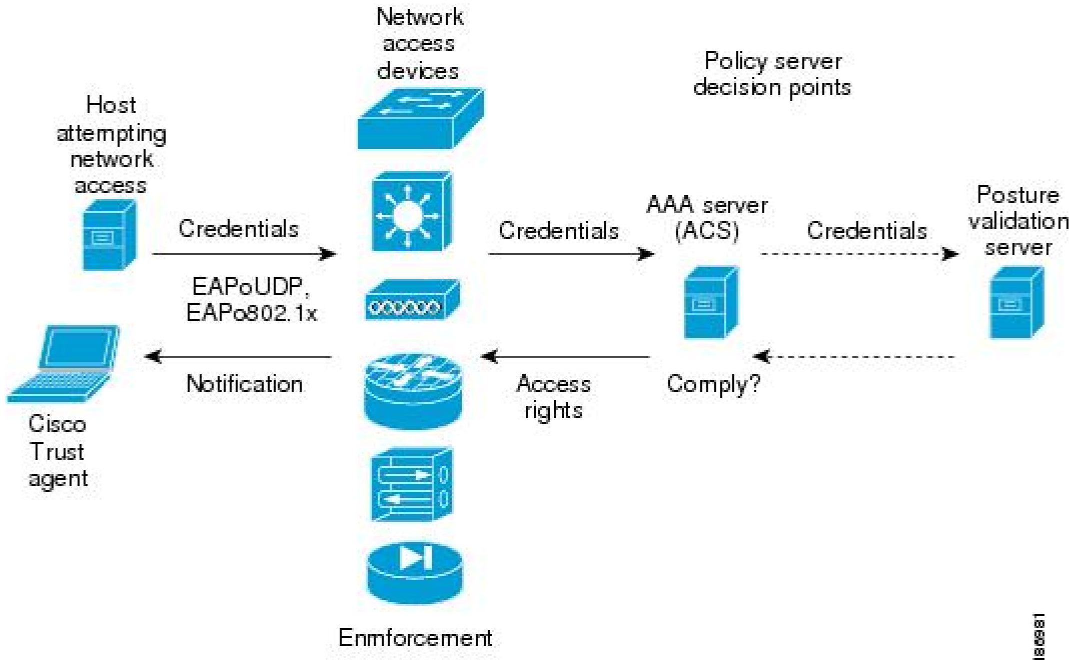
Third-party server that acts as an application-specific policy decision point in NAC for authorizing a set of posture credentials against a set of policy rules. The posture validation server receives requests from an authentication server.

NAC Posture Validation

Posture validation occurs when a NAC-enabled NAD detects an endpoint device that is attempting to connect or use its network resources. When the NAD detects a new endpoint device, it requests the network access profile for the endpoint device from an AAA server (such as the Cisco Secure ACS).

Figure 9: NAC Endpoint Device Posture Validation

This figure shows the NAC endpoint device posture validation



process.

The AAA server determines if the endpoint device has a posture agent installed. If the endpoint device has a posture agent (such as the Cisco Trust Agent), the AAA server requests the endpoint device for posture information via the NAD. The endpoint device responds to the AAA server with a set of posture credentials. The AAA server then validates the posture information locally or delegates the posture validation decisions to one or more external posture validation servers.

If the endpoint device does not have a posture agent, the AAA server may request an audit server to collect posture information from the device through other means (for example, fingerprinting and port scanning). The AAA server also asks the audit server to validate that information and return a posture validation decision.

The AAA server aggregates the posture validation results from these sources and makes an authorization decision that is based on whether the endpoint device complies with the network policy. The AAA server determines the network access profile for the endpoint device and sends the profile to the NAD for enforcement of the endpoint device authorization.

The examination of endpoint device credentials by the AAA server can result in one or more application posture tokens (APTs). An APT represents a compliance check for a given vendor's application. The AAA server aggregates all APTs from the posture validation servers into a single system posture token (SPT) that represents the overall compliance of the endpoint device. The value SPT is based on the worst APT from the set of APTs. Both APTs and SPTs are represented using the following predefined tokens:

Healthy
: The endpoint device complies with the posture policy so no restrictions are placed on this device.

Checkup
: The endpoint device is within policy but does not have the latest software; an update is recommended.

Transition
: The endpoint device is in the process of having its posture checked and is given interim access pending a result from a complete posture validation. A transition result may occur when a host is booting and complete posture information is not available, or when complete audit results are not available.

Quarantine
: The endpoint device is out of compliance and must be restricted to a quarantine network for remediation. This device is not actively placing a threat on other endpoint devices but is vulnerable to attack or infection and must be updated as soon as possible.

Infected
: The endpoint device is an active threat to other endpoint devices; network access must be severely restricted and the endpoint device must be placed into remediation or denied all network access to the endpoint device.

Unknown
: The AAA server cannot determine the posture credentials of the endpoint device. You need to determine the integrity of the endpoint device so that proper posture credentials can be attained and assessed for network access authorization.

IP Device Tracking

The IP device tracking allows endpoint devices to remain connected to the network if the AAA server is not available. Typical deployments of NAC use Cisco Secure ACS to validate the client posture and to pass policies back to the NAD.

IP device tracking provides the following benefits:

- While AAA is unavailable, the endpoint device still has connectivity to the network, although it may be restricted.
- When the AAA server is available again, a user can be revalidated and the user's policies can be downloaded from the ACS.

Note When the AAA server is down, the NAD applies the IP device tracking policy only if there is no existing policy associated with the host. Typically, during revalidation when the AAA server goes down, the NAD retains the current policies used for the endpoint device.

NAC LPIP

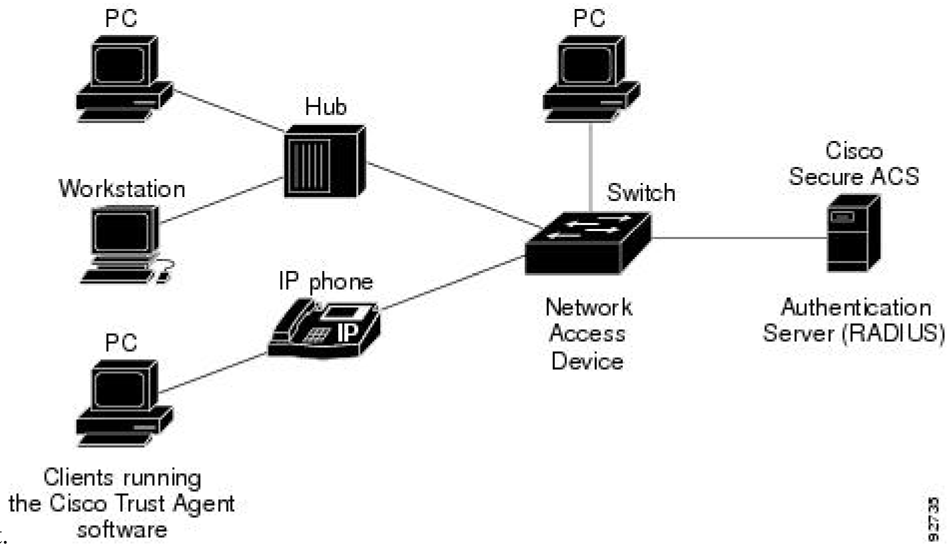
NAC LAN port IP (LPIP) validation uses the Layer 3 transport EAPoUDP to carry posture validation information. LPIP validation has the following characteristics:

- Operates only on Layer 2 ports and cannot operate on Layer 3 ports.
- Subjects all hosts sending IP traffic on the port to posture validation.

LPIP validation triggers admission control by snooping on DHCP messages or Address Resolution Protocol (ARP) messages rather than intercepting IP packets on the data path. LPIP validation performs policy enforcement using access control lists (ACLs).

Figure 10: Network Using LPIP Validation

This figure shows the LPIP validation process for a single host connected to a NAD port or multiple hosts on the same NAD port.



When you enable LPIP validation, EAPoUDP only supports IPv4 traffic. The NAD checks the antivirus status of the endpoint devices or clients and enforces access control policies.

Posture Validation

When you enable LPIP validation on a port connected to one or more endpoint devices, the Cisco NX-OS device uses DHCP snooping and ARP snooping to identify connected hosts. The Cisco NX-OS device initiates posture validation after receiving an ARP packet or creating a DHCP snooping binding entry. ARP snooping is the default method to detect connected hosts. If you want the NAD to detect hosts when a DHCP snooping binding entry is created, you must enable DHCP snooping.

Admission Triggers

ARP snooping allows LPIP validation to detect hosts with either dynamically acquired or statically configured IP addresses. When the NAD receives an ARP packet from an unknown host, it triggers posture validation. If you have enabled DHCP snooping on the interface, the creation of a DHCP binding entry on the NAD triggers posture validation. DHCP snooping provides a slightly faster response time because DHCP packets are exchanged prior to sending ARP requests. Both ARP snooping and DHCP snooping can trigger posture validation on the same host. In this case, the trigger initiated by the creation of a DHCP snooping binding takes precedence over ARP snooping.

Note When you use DHCP snooping and ARP snooping to detect the presence of a host, a malicious host might set up a static ARP table to bypass posture validation. To protect against this type of exposure, you can enable IP Source Guard on the port. IP Source Guard prevents unauthorized hosts from accessing the network.

Posture Validation Methods

After posture validation is triggered for a host, you can use one of two possible methods to determine the policy to be applied for the host:

- Exception lists
- EAPoUDP

Exception Lists

An exception list contains local profile and policy configurations. Use the identity profile to statically authorize or validate devices based on the IP address and MAC address. You can associate an identity profile with a local policy that specifies the access control attributes.

Using an exception list, you can bypass posture validation for specific endpoint devices and apply a statically configured policy. After posture validation is triggered, the NAD checks for the host information in the exception list. If a match is found in the exception list, the NAD applies the configured policy for the endpoint device.

EAPoUDP

If an endpoint device does not match the exception list, the NAD sends an EAPoUDP packet to initiate posture validation. While posture validation occurs, the NAD enforces the default access policy. After the NAD sends an EAPoUDP message to the host and the host responds to the antivirus condition request, the NAD forwards the EAPoUDP response to the Cisco Secure ACS. If the NAD does not receive a response from the host after the specified number of attempts, the NAD classifies the host as nonresponsive. After the ACS validates the credentials, the authentication server returns an Access-Accept or Access-Reject message to the NAD. The NAD updates the EAPoUDP session table and enforces the access limitations, which segments and quarantines the poorly postured endpoint device or denies network access.

Note An Access-Reject message indicates that the EAPoUDP exchange has failed. This message does not indicate that the endpoint device is poorly postured.

For an Access-Accept message, the NAD applies the enforcement policy that contains the policy-based ACL (PACL) name and starts the EAP revalidation and status query timers.

For an Access-Reject message, the NAD removes any enforcement policy for the host and puts the endpoint device into the Held state for a configured period of time (Hold timer). After the Hold timer expires, the NAD revalidates the endpoint device.

Note If you delete a DHCP snooping binding entry for an endpoint device, the NAD removes the client entry in the session table and the client is no longer authenticated.

Policy Enforcement Using ACLs

LPIP validation uses PACLs for policy enforcement.

The NAD applies the PACL when the posture validation fails (the AAA server sends an Access-Reject message). The default policy is to use the active MAC ACL applied to the port (also called a port ACL [PACL]). The active MAC ACL could either be a statically configured PACL or an AAA server-specified PACL based on 802.1X authentication.

The PACL defines a group that expands to a list of endpoint device IP addresses. The PACLs usually contain the endpoint device IP addresses. Once the NAD classifies an endpoint device using a particular group, the

NAD adds the IP address that corresponds to the endpoint device to the appropriate group. The result is that the policy is applied to the endpoint device.

When you configure LPIP validation for an NAD port, you must also configure a default PACL on that NAD port. In addition, you should apply the default ACL to the IP traffic for hosts that have not completed posture validation.

If you configure the default ACL on the NAD and the Cisco Secure ACS sends a host access policy to the NAD, the NAD applies the policy to that traffic from the host that is connected to a NAD port. If the policy applies to the traffic, the NAD forwards the traffic. If the policy does not apply, the NAD applies the default ACL. However, if the NAD gets an endpoint device access policy from the Cisco Secure ACS but the default ACL is not configured, the LPIP validation configuration does not take effect.

Note Both DHCP snooping and ARP snooping are enabled per VLAN. However, security ACLs downloaded as a result of NAC Layer 2 posture validation are applied per port. As a result, all DHCP and ARP packets are intercepted when these features are enabled on any VLAN.

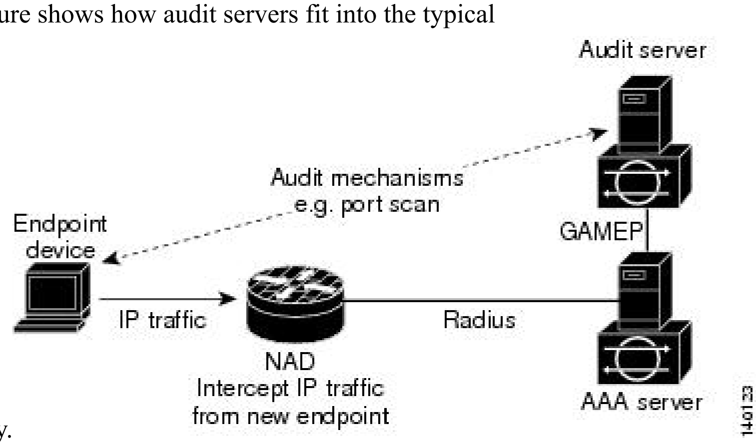
Audit Servers and Nonresponsive Hosts

Endpoint devices that do not run a posture agent (Cisco Trust Agent) cannot provide credentials when challenged by NADs. These devices are described as *agentless* or *nonresponsive*.

The NAC architecture supports audit servers to validate agentless endpoint devices. An audit server is a third-party server that can probe, scan, and determine security compliance of a host without needing a posture again on the endpoint device. The result of the audit server examination can influence the access servers to make network access policy decisions specific to the endpoint device instead of enforcing a common restrictive policy for all nonresponsive endpoint devices. You can build more robust host audit and examination functionality by integrating any third-party audit operations into the NAC architecture.

Figure 11: NAC Device Roles

This figure shows how audit servers fit into the typical



topology.

NAC assumes that the audit server can be reached so that the endpoint device can communicate with it. When an endpoint device makes network access through the NAD configured for posture validation, the network access device eventually requests the AAA server (Cisco Secure ACS) for an access policy to be enforced for the host. The AAA server can be configured to trigger a scan of the host with an external audit server. The audit server scan occurs asynchronously and takes several seconds to complete. During the scan, the AAA server conveys a minimal restrictive security policy to NAD for enforcement along with a short poll timer (session-timeout). The NAD polls the AAA sever at the specified timer interval until the result is available from the audit server. After the AAA server receives the audit result, it computes an access policy based on the audit result and sends it to the NAD for enforcement on its next request.

NAC Timers

This section describes the NAC timers.

Hold Timer

The hold timer prevents a new EAPoUDP session from immediately starting after the previous attempt to validate that the session fails. NAC uses this time only when the Cisco Secure ACS sends an Accept-Reject message to the NAD. The default value of the hold timer is 180 seconds (3 minutes).

An EAPoUDP session might not be validated when the posture validation of the host fails, a session timer expires, or the NAD or Cisco Secure ACS receives invalid messages. If the NAD or authentication server continuously receives invalid messages, a malicious user might be trying to cause a denial-of-service attack.

AAA Timer

The AAA timer controls the amount of time that the NAD waits for a response from the AAA server before resending a request during posture validation. The default value of the retransmission timer is 60 seconds.

Note Setting the timer value too low might cause unnecessary transmissions; setting the timer value too high might cause poor response times.

Retransmit Timer

The retransmit timer controls the amount of time that the NAD waits for a response from the client before resending a request during posture validation. The default value of the retransmission timer is 3 seconds.

Note Setting the timer value too low might cause unnecessary transmissions; setting the timer value too high might cause poor response times.

Revalidation Timer

The revalidation timer controls the amount of time that the NAD applies a NAC policy to an endpoint device that used EAPoUDP messages during posture validation. The timer starts after the initial posture validation completes. The timer resets when the host is revalidated. The default value of the revalidation timer is 36000 seconds (10 hours).

The Cisco NX-OS software bases the revalidation timer operation on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS-REQUEST attribute (Attribute[29]) in the Access-Accept message from the AAA server (Cisco Secure ACS). If the NAD receives the Session-Timeout value, this value overrides the revalidation timer value on the NAD.

If the revalidation timer expires, the NAD action depends on one of these values of the Termination-Action attribute:

- If the value of the Termination-Action RADIUS attribute is the default, the session ends.

- If the NAD receives a value for the Termination-Action attribute other than the default, the EAPoUDP session and the current access policy remain in effect during posture revalidation.
- If the value of the Termination-Action attribute is RADIUS, the NAD revalidates the client.
- If the packet from the server does not include the Termination-Action attribute, the EAPoUDP session ends.

Status-Query Timer

The status-query timer controls the amount of time that the NAD waits before verifying that the previously validated client is present and that its posture has not changed. Only clients that were authenticated with EAPoUDP messages use this timer, which starts after the client is initially validated. The default value of the status-query timer is 300 seconds (5 minutes).

The timer resets when the host is reauthenticated. When the timer expires, the NAD checks the host posture validation by sending a Status-Query message to the host. If the host sends a message to the NAD that the posture has changed, the NAD revalidates the posture of the host.

NAC Posture Validation and Redundant Supervisor Modules

When a switchover occurs, the Cisco NX-OS device maintains information about the endpoint devices and the current PACL application but loses the current state of each EAPoUDP session. The Cisco NX-OS device removes the current PACL application and restarts posture validation.

LPIP Validation and Other Security Features

This section describes how LPIP validation interacts with other security features on the Cisco NX-OS device.

802.1X

If you configure both 802.1X and LPIP on a port, the traffic that does not pass the 802.1X-authenticated source MAC check does not trigger posture validation. When you configure 802.1X on a port, the port cannot transmit or receive traffic (other than EAP over LAN [EAPOL] frames) until the attached host is authenticated via 802.1X. This mechanism ensures that the IP traffic from the host does not trigger posture validation before it is authenticated.

Port Security

The NAD checks the source MAC against the port security MACs and drops the endpoint device if the check fails. The NAD allows posture validation only on port security-validated MAC addresses. If a port security violation occurs and results in a port shutdown, the Cisco NX-OS software removes the LPIP state of the port.

DHCP Snooping

Posture validation does not occur until after a DHCP creates a binding entry. When you enable DHCP snooping and LPIP, the Cisco NX-OS software triggers posture validation for a host when DHCP creates a binding entry for the host using DHCP to acquire IP address.

Dynamic ARP Inspection

If you enable LPIP validation on the interface, posture validation is triggered only if the packet passes the dynamic ARP inspection (DAI) check. If you do not enable DAI, then all ARP packets (with valid MAC/IP pairs) will trigger posture validation.

Note ARP snooping is the default mechanism of detecting hosts. However, ARP snooping is not the same as DAI. If you enable LPIP validation, the Cisco NX-OS software passes the ARP packets to LPIP validation. If you enable DAI, the Cisco NX-OS software passes the ARP packets to DAI.

Note If you have enabled DHCP snooping, the Cisco NX-OS software bypasses DAI.

IP Source Guard

IP Source Guard is a per-interface traffic filter that permits IP traffic only when the IP address and MAC address of each packet matches one of two sources of IP and MAC address bindings:

- Entries in the DHCP snooping binding table.
- Static IP source entries that you configure.

Filtering on trusted IP and MAC address bindings helps prevent attacks that rely on spoofing the IP address of a valid host. To circumvent IP Source Guard, an attacker would have to spoof both the IP address and the MAC address of a valid host.

Posture Host-Specific ACEs

The Cisco NX-OS software drops the packet if the packet matches the deny condition and skips the active PACL if a packet matches a permit condition. If no implicit deny exists at the end of the ACEs and no match occurs, the Cisco NX-OS software checks the packet against the active PACL.

Note If you enable DHCP snooping or DAI, the NAD does not process posture host-specific ACEs.

Active PACLs

The active PACL is either a statically configured PACL or an AAA server-specified PACL that is based on 802.1X authentication. The packet is dropped if it matches any deny condition and moves to the next step if it matches a permit condition.

Note If you have enabled DHCP snooping or DAI, the NAD does not process the active PACL.

VACLs

The Cisco NX-OS software drops any packet that matches a deny condition.

Note If you have enabled DHCP snooping or DAI, the NAD bypasses the VACLs.

Virtualization Support for NAC

NAC configuration and operation are local to the virtual device context (VDC).

For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Prerequisites for NAC

NAC has the following prerequisites:

- Ensure that a Layer 3 route exists between the NAD and each endpoint device.

NAC Guidelines and Limitations

NAC has the following guidelines and limitations:

- EAPoUDP bypass and AAA down policy are not supported.
- NAC uses only RADIUS for authentication.

LPIP Limitations

LPIP validation has the following limitations:

- LPIP validation is allowed only on access ports.
- You cannot enable LPIP validation on trunk ports or port channels.
- LPIP validation is not allowed on ports that are SPAN destinations.
- LPIP validation is not allowed on ports that are part of a private VLAN.
- LPIP validation does not support IPv6.
- LPIP validation is allowed only for endpoint devices directly connected to the NAD.
- You cannot use LPIP validation unless you have a Layer 3 route between the NAD and the endpoint device.

Default Settings for NAC

This table lists the default settings for NAC parameters.

Table 22: Default NAC Parameter Settings

Parameters	Default
EAPoUDP	Disabled.
EAP UDP port number	21862 (0x5566).
Clientless hosts allowed	Disabled.
Automatic periodic revalidation	Enabled.
Revalidation timeout interval	36000 seconds (10 hours).
Retransmit timeout interval	3 seconds.
Status query timeout interval	300 seconds (5 minutes).
Hold timeout interval	180 seconds (3 minutes).
AAA timeout interval	60 seconds (1 minute).
Maximum retries	3.
EAPoUDP rate limit maximum	20 simultaneous sessions.
EAPoUDP logging	Disabled.
IP device tracking	Enabled.

Configuring NAC

This section describes how to configure NAC.

Note 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.

Process for Configuring NAC

Follow these steps to configure NAC:

SUMMARY STEPS

1. Enable EAPoUDP.
2. Configure the connection to the AAA server.
3. Apply PACLs to the interfaces connected to endpoint devices.
4. Enable NAC on the interfaces connected to the endpoint devices.

DETAILED STEPS

Step 1 Enable EAPoUDP.

Step 2 Configure the connection to the AAA server.

Step 3 Apply PACLs to the interfaces connected to endpoint devices.

Step 4 Enable NAC on the interfaces connected to the endpoint devices.

Related Topics

Enabling EAPoUDP, on page 310
Enabling the Default AAA Authenication Method for EAPoUDP, on page 311
Applying PACLs to Interfaces, on page 312
Enabling NAC on an Interface, on page 313

Enabling EAPoUDP

The Cisco NX-OS device relays Extensible Authentication Protocol (EAP) messages between the endpoints and the authentication server. You must enable EAP over UDP (EAPoUDP) before configuring NAC on the Cisco NX-OS device.

SUMMARY STEPS

1. **configure terminal**
2. **feature eou**
3. **exit**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**feature eou** **Example:** `switch(config)# feature eou`	Enables EAPoUDP. The default is disabled.

	Command or Action	Purpose

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

Step 4	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling the Default AAA Authenication Method for EAPoUDP

You must enable the default AAA authentication method EAPoUDP.

> **Note** LPIP can use only RADIUS for authentication.

Before you begin

Enable EAPoUDP.

Configure RADIUS or TACACS+ server groups, as needed.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication eou default group** *group-list*
3. **exit**
4. (Optional) **show aaa authentication**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**aaa authentication eou default group** *group-list* **Example:** `switch(config)# aaa authentication eou default group RadServer`	Configures a list of one or more RADIUS server groups as the default AAA authentication method for EAPoUDP. The *group-list* argument consists of a space-delimited list of groups. The group names are as follows: • **radius**—Uses the global pool of RADIUS servers for authentication.

	Command or Action	Purpose
		• *named-group*—Uses a named subset of RADIUS servers for authentication. The default setting is no method.

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

Step 4	(Optional) **show aaa authentication** **Example:** `switch# show aaa authentication`	Displays the default AAA authentication methods.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310
Configuring AAA, on page 25
Configuring RADIUS, on page 61

Applying PACLs to Interfaces

You must apply a PACL to the access interfaces on the NAD that perform LPIP posture validation if no PACL is available from the AAA server.

Before you begin

Create a MAC ACL.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **mac access-group** *access-list*
4. **exit**
5. (Optional) **show running-config interface**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies the Ethernet interface and enters interface configuration mode.

Step 3	**mac access-group** *access-list* **Example:** `switch(config-if)# mac access-group acl-01`	Applies a PACL to the interface for traffic that flows in the direction specified. **Note** An interface can have only one PACL. To replace the PACL on the interface, enter this command again using the new PACL name.

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits global configuration mode.

Step 5	(Optional) **show running-config interface** **Example:** `switch(config)# show running-config interface`	Displays the interface PACL 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.

Enabling NAC on an Interface

You must enable NAC on an interface for posture validation to occur.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **switchport**
4. **switchport mode access**
5. **nac enable**
6. **exit**
7. (Optional) **show running-config interface**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port*
	
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies the Ethernet interface and enters interface configuration mode.

Step 3	**switchport** **Example:** `switch(config-if)# switchport`	Sets the interface as a Layer 2 switching interface. By default, all ports are Layer 3 ports.
Step 4	**switchport mode access** **Example:** `switch(config-if)# switchport mode access`	Configures the port mode as access.
Step 5	**nac enable** **Example:** `switch(config-if)# nac enable`	Enables NAC on the interface.

Step 6	**exit**
	
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits global configuration mode.

Step 7	(Optional) **show running-config interface** **Example:** `switch(config)# show running-config interface`	Displays the interface PACL configuration.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310

Configuring Identity Policies and Identity Profile Entries

You can use the identity profile to configure exceptions to LPIP posture validation. The identity profile contains entries for the endpoint devices for which are not subject to LPIP validation. You can optionally configure an identity policy for each identity profile entry that specifies a PACL that the NX-OS device applies to the endpoint device. The default identity policy is the PACL for the interface.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **identity policy** *policy-name*
3. **object-group** *access-list*
4. (Optional) **description "** *text* **"**
5. **exit**
6. (Optional) **show identity policy**
7. **identity profile eapoudp**
8. **device** {**authenticate** | **not-authenticate**} {**ip-address** *ipv4-address* [*ipv4-subnet-mask*] | **mac-address** *mac-address* [*mac-subnet-mask*]} **policy** *name*
9. **exit**
10. (Optional) **show identity profile eapoudp**
11. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**identity policy** *policy-name*
	Example:
	`switch(config)# identity policy AccType1`
	`switch(config-id-policy)#`
		Specifies the identity policy name and enters identity policy configuration mode. You can create a maximum of 1024 identity policies. The maximum length of the name is 100 characters.

Step 3	**object-group** *access-list* **Example:** `switch(config-id-policy)# object-group maxaclx`	Specifies the IP ACL or MAC ACL for the policy.
Step 4	(Optional) **description "** *text* **"** **Example:** `switch(config-id-policy)# description "This policy prevents endpoint device without a PA"`	Provides a description for the identity policy. The maximum length is 100 characters.

Step 5	**exit**
	Example:
	`switch(config-id-policy)# exit`
	`switch(config)#`
		Exits identity policy configuration mode.

Step 6	(Optional) **show identity policy** **Example:**	Displays the identity policy configuration.

	Command or Action	Purpose
	`switch(config)# show identity policy`	

Step 7	**identity profile eapoudp**
	Example:
	`switch(config)# identity profile eapoudp`
	`switch(config-id-prof)#`
		Enters identity profile configuration mode for EAPoUDP.

Step 8	**device** {**authenticate** | **not-authenticate**} {**ip-address** *ipv4-address* [*ipv4-subnet-mask*] | **mac-address** *mac-address* [*mac-subnet-mask*]} **policy** *name* **Example:** `switch(config-id-prof)# device authenticate ip-address 10.10.2.2 policy AccType1`	Specifies an exception entry. The maximum number of entries is 5000.

Step 9	**exit**
	Example:
	`switch(config-id-prof)# exit`
	`switch(config)#`
		Exits identity profile configuration mode.

Step 10	(Optional) **show identity profile eapoudp** **Example:** `switch(config)# show identity profile eapoudp`	Displays the identity profile configuration.
Step 11	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310

Allowing Clientless Endpoint Devices

You can allow posture validation endpoint devices in your network that do not have a posture agent installed (clientless). The posture validation is performed by an audit server that has access to the endpoint devices.

Before you begin

Enable EAPoUDP.

Verify that the AAA server and clientless endpoint devices can access the audit server.

SUMMARY STEPS

1. **configure terminal**
2. **eou allow clientless**
3. **exit**
4. (Optional) **show eou**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**eou allow clientless** **Example:** `switch(config)# eou allow clientless`	Allows posture validation for clientless endpoint devices. The default is disabled.

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

Step 4	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310

Enabling Logging for EAPoUDP

You can enable logging for EAPoUDP event messages. EAPoUDP events include errors and status changes. The destination for these event messages is the configured syslog.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **eou logging**
3. **exit**
4. (Optional) **show eou**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**eou logging** **Example:** `switch(config)# eou logging`	Enables EAPoUDP logging. The default is disabled.

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

Step 4	(Optional) **show eou** **Example:** `switch)# show eou`	Displays the EAPoUDP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310

Changing the Global EAPoUDP Maximum Retry Value

You can change the global maximum number of EAPoUDP retries. The default value is three.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **eou max-retry** *count*
3. **exit**
4. (Optional) **show eou**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**eou max-retry** *count* **Example:** `switch(config)# eou max-retry 2`	Changes the EAPoUDP maximum retry count. The default is 3. The range is from 1 to 3.

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

Step 4	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310
Changing the EAPoUDP Maximum Retry Value for an Interface, on page 319

Changing the EAPoUDP Maximum Retry Value for an Interface

You can change the maximum number of EAPoUDP retries for an interface. The default value is three.

Before you begin

Enable EAPoUDP.

Enable NAC on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **eou max-retry** *count*
4. **exit**
5. (Optional) **show eou**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies the Ethernet interface and enters interface configuration mode.

Step 3	**eou max-retry** *count* **Example:** `switch(config-if)# eou max-retry 2`	Changes the EAPoUDP maximum retry count. The default is 3. The range is from 1 to 3.

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 5	(Optional) **show eou** **Example:** `switch(config)# show eou`	Displays the EAPoUDP 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.

Related Topics

Enabling EAPoUDP, on page 310
Changing the Global EAPoUDP Maximum Retry Value, on page 318
Enabling NAC on an Interface, on page 313

Changing the UDP Port for EAPoUDP

You can change the UDP port used by EAPoUDP. The default port is 21862.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **eou port** *udp-port*
3. **exit**

4. (Optional) **show eou**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**eou port** *udp-port* **Example:** `switch(config)# eou port 27180`	Changes the UDP port used by EAPoUDP. The default is 21862. The range is from 1 to 65535.

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

Step 4	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310

Configuring Rate Limiting of Simultaneous EAPoUDP Posture Validation Sessions

You can configure rate limiting to control the number of simultaneous EAPoUDP posture validations sessions. You can change the rate-limiting value that controls the maximum number of simultaneous EAPoUDP posture validation sessions. The default number is 20. Setting the number to zero (0) disables rate limiting.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **eou ratelimit** *number-of-sessions*
3. **exit**

4. (Optional) **show eou**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**eou ratelimit** *number-of-sessions* **Example:** `switch(config)# eou ratelimit 15`	Configures the number of simultaneous EAPoUDP posture validation sessions. The default is 20. The range is from 0 to 200. **Note** A setting of zero (0) disables rate limiting.

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

Step 4	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310

Configuring Global Automatic Posture Revalidation

The Cisco NX-OS software automatically revalidates the posture of the endpoint devices for the Cisco NX-OS device at a configured interval. The default interval is 36,000 seconds (10 hours). You can disable revalidation or change the length of the revalidation interval.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **eou revalidate**
3. (Optional) **eou timeout revalidation** *seconds*

4. **exit**
5. (Optional) **show eou**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **eou revalidate** **Example:** `switch(config)# eou revalidate`	Enables the automatic posture validation. The default is enabled.
Step 3	(Optional) **eou timeout revalidation** *seconds* **Example:** `switch(config)# eou timeout revalidation 30000`	Changes the revalidation timer interval. The default is 36000. The range is from 5 to 86400 seconds. Use the **no eou revalidate** command to disable automatic posture validation.

Step 4	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 5	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310
Configuring Automatic Posture Revalidation for an Interface, on page 323

Configuring Automatic Posture Revalidation for an Interface

The Cisco NX-OS software automatically revalidates the posture of the endpoint devices for the Cisco NX-OS device at a configured interval. The default interval is 36,000 seconds (10 hours). You can disable revalidation or change the length of the revalidation interval.

Before you begin

Enable EAPoUDP.

Enable NAC on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. (Optional) **eou revalidate**
4. (Optional) **eou timeout revalidation** *seconds*
5. **exit**
6. (Optional) **show eou**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot*/*port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies the Ethernet interface and enters interface configuration mode.

Step 3	(Optional) **eou revalidate** **Example:** `switch(config-if)# eou revalidate`	Enables the automatic posture validation. The default is enabled. Use the **no eou revalidate** command to disable automatic posture validation.
Step 4	(Optional) **eou timeout revalidation** *seconds* **Example:** `switch(config-if)# eou timeout revalidation 30000`	Changes the revalidation timer interval. The default is 36000. The range is from 5 to 86400 seconds.

Step 5	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits global configuration mode.

Step 6	(Optional) **show eou** **Example:** `switch(config)# show eou`	Displays the EAPoUDP configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310
Configuring Global Automatic Posture Revalidation, on page 322
Enabling NAC on an Interface, on page 313

Changing the Global EAPoUDP Timers

The Cisco NX-OS software supports the following global timers for EAPoUDP:

AAA
: Controls the amount of time that the NAD waits for a response from the AAA server before resending a request during posture validation.

Hold period
: Prevents a new EAPoUDP session from immediately starting after the previous attempt to validate that the session fails. NAC uses this time only when the Cisco Secure ACS sends an Accept-Reject message to the NAD.

Retransmit
: Controls the amount of time that the NAD waits for a response from the client before resending a request during posture validation.

Revalidation
: Controls the amount of time that the NAD applies a NAC policy to an endpoint device that used EAPoUDP messages during posture validation. The timer starts after the initial posture validation completes.

Status query
: Controls the amount of time that the NAD waits before verifying that the previously validated client is present and that its posture has not changed. Only clients that were authenticated with EAPoUDP messages use this timer, which starts after the client is initially validated.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **eou timeout aaa** *seconds*
3. (Optional) **eou timeout hold-period** *seconds*
4. (Optional) **eou timeout retransmit** *seconds*
5. (Optional) **eou timeout revalidation** *seconds*
6. (Optional) **eou timeout status-query** *seconds*
7. **exit**
8. (Optional) **show eou**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
Step 2	(Optional) **eou timeout aaa** *seconds* **Example:** `switch(config)# eou timeout aaa 30`	Changes the AAA timeout interval. The default is 60 seconds (1 minute). The range is from 0 to 60 seconds.
Step 3	(Optional) **eou timeout hold-period** *seconds* **Example:** `switch(config)# eou timeout hold-period 300`	Changes the hold period timeout interval. The default is 180 seconds (3 minutes). The range is from 60 to 86400 seconds.
Step 4	(Optional) **eou timeout retransmit** *seconds* **Example:** `switch(config)# eou timeout retransmit 10`	Changes the retransmit timeout interval. The default is 3 seconds. The range is from 1 to 60 seconds.
Step 5	(Optional) **eou timeout revalidation** *seconds* **Example:** `switch(config)# eou timeout revalidation 30000`	Changes the revalidation timer interval. The default is 36000. The range is from 5 to 86400 seconds.
Step 6	(Optional) **eou timeout status-query** *seconds* **Example:** `switch(config)# eou timeout status-query 360`	Changes the status query timeout interval. The default is 300 seconds (5 minutes). The range is from 10 to 1800 seconds.

Step 7	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 8	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310
Changing the EAPoUDP Timers for an Interface, on page 326
NAC Timers, on page 305

Changing the EAPoUDP Timers for an Interface

The Cisco NX-OS software supports the following timers for EAPoUDP for each interface enabled for NAC:

AAA

Controls the amount of time that the NAD waits for a response from the AAA server before resending a request during posture validation.

Hold period

Prevents a new EAPoUDP session from immediately starting after the previous attempt to validate that the session fails. NAC uses this time only when the Cisco Secure ACS sends an Accept-Reject message to the NAD.

Retransmit

Controls the amount of time that the NAD waits for a response from the client before resending a request during posture validation.

Revalidation

Controls the amount of time that the NAD applies a NAC policy to an endpoint device that used EAPoUDP messages during posture validation. The timer starts after the initial posture validation completes.

Status query

Controls the amount of time that the NAD waits before verifying that the previously validated client is present and that its posture has not changed. Only clients that were authenticated with EAPoUDP messages use this timer, which starts after the client is initially validated.

Before you begin

Enable EAPoUDP.

Enable NAC on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. (Optional) **eou timeout aaa** *seconds*
4. (Optional) **eou timeout hold-period** *seconds*
5. (Optional) **eou timeout retransmit** *seconds*
6. (Optional) **eou timeout revalidation** *seconds*
7. (Optional) **eou timeout status-query** *seconds*
8. **exit**
9. (Optional) **show eou**
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies the Ethernet interface and enters interface configuration mode.

Step 3	(Optional) **eou timeout aaa** *seconds* **Example:** `switch(config-if)# eou timeout aaa 50`	Changes the AAA timeout interval. The default is 60 seconds (1 minute). The range is from 0 to 60 seconds.
Step 4	(Optional) **eou timeout hold-period** *seconds* **Example:** `switch(config-if)# eou timeout hold-period 300`	Changes the hold period timeout interval. The default is 180 seconds (3 minutes). The range is from 60 to 86400 seconds.
Step 5	(Optional) **eou timeout retransmit** *seconds* **Example:** `switch(config-if)# eou timeout retransmit 10`	Changes the retransmit timeout interval. The default is 3 seconds. The range is from 1 to 60 seconds.
Step 6	(Optional) **eou timeout revalidation** *seconds* **Example:** `switch(config-if)# eou timeout revalidation 30000`	Changes the revalidation timer interval. The default is 36000. The range is from 5 to 86400 seconds.
Step 7	(Optional) **eou timeout status-query** *seconds* **Example:** `switch(config-if)# eou timeout status-query 360`	Changes the status query timeout interval. The default is 300 seconds (5 minutes). The range is from 10 to 1800 seconds.

Step 8	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 9	(Optional) **show eou** **Example:** `switch(config)# show eou`	Displays the EAPoUDP configuration.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310
Changing the Global EAPoUDP Timers, on page 325
NAC Timers, on page 305
Enabling NAC on an Interface, on page 313

Resetting the EAPoUDP Global Configuration to the Default Values

You can reset the EAPoUDP global configuration to the default values.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **eou default**
3. **exit**
4. (Optional) **show eou**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**eou default** **Example:** `switch(config)# eou default`	Resets the EAPoUDP configuration to the default values.

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

Step 4	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310
Resetting the EAPoUDP Interface Configuration to the Default Values, on page 330

Resetting the EAPoUDP Interface Configuration to the Default Values

You can reset the EAPoUDP configuration for an interface to the default values.

Before you begin

Enable EAPoUDP.

Enabled NAC on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **eou default**
4. **exit**
5. (Optional) **show eou interface ethernet** *slot*/*port*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot*/*port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies the Ethernet interface and enters interface configuration mode.

Step 3	**eou default** **Example:** `switch(config-if)# eou default`	Resets the EAPoUDP configuration for the interface to the default values.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits interface configuration mode.

Step 5	(Optional) **show eou interface ethernet** *slot*/*port* **Example:** `switch(config)# show eou interface ethernet 2/1`	Displays the EAPoUDP 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.

Related Topics

Enabling EAPoUDP, on page 310
Resetting the EAPoUDP Global Configuration to the Default Values, on page 329
Enabling NAC on an Interface, on page 313

Configuring IP Device Tracking

You can configure IP device tracking. The process for the IP device tracking for AAA servers operates is as follows:

- The Cisco NX-OS device detects a new session.
- Before posture validation is triggered and if the AAA server is unreachable, the Cisco NX-OS device applies the IP device tracking policy and maintains the session state as AAA DOWN.
- When the AAA server is once again available, a revalidation occurs for the host.

Note When the AAA server is down, the Cisco NX-OS device applies the IP device tracking policy only if no existing policy is associated with the endpoint device. During revalidation when the AAA server goes down, the Cisco NX-OS device retains the policies that are used for the endpoint device.

SUMMARY STEPS

1. **configure terminal**
2. **ip device tracking enable**
3. (Optional) **ip device tracking probe** {**count** *count* | **interval** *seconds*}
4. (Optional) **radius-server host** {*hostname* | *ip-address*} **test** [**username** *username* [**password** *password*]] [**idle-time** *minutes*]
5. **exit**
6. (Optional) **show ip device tracking all**
7. (Optional) **show radius-server** {*hostname* | *ip-address*}
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip device tracking enable** **Example:** `switch(config)# ip device tracking enable`	Enables the IP device tracking. The default state is enabled.

	Command or Action	Purpose
Step 3	(Optional) **ip device tracking probe** {**count** *count* | **interval** *seconds*} **Example:** `switch(config)# ip device tracking probe count 4`	Configures these parameters for the IP device tracking table: **count** Sets the number of times that the Cisco NX-OS device sends the ARP probe. The range is from 1 to 5. The default is 3. **interval** Sets the number of seconds that the Cisco NX-OS device waits for a response before resending the ARP probe. The range is from 1 to 302300 seconds. The default is 30 seconds
Step 4	(Optional) **radius-server host** {*hostname* | *ip-address*} **test** [**username** *username* [**password** *password*]] [**idle-time** *minutes*] **Example:** `switch(config)# radius-server host 10.10.1.1 test username User2 password G1r2D37&k idle-time 5`	Configures RADIUS server test packet parameters. The default username is test and the default password is test. The **idle-time** parameter determines how often the server is tested to determine its operational status. If there is no traffic to the RADIUS server, the NAD sends dummy packets to the RADIUS server based on the idle timer value. The default value for the idle timer is 0 minutes (disabled). If you have multiple RADIUS servers, reenter this command.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 6	(Optional) **show ip device tracking all** **Example:** `switch# show ip device tracking all`	Displays IP device tracking information.
Step 7	(Optional) **show radius-server** {*hostname* | *ip-address*} **Example:** `switch# show radius-server 10.10.1.1`	Displays RADIUS server information.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 310

Clearing IP Device Tracking Information

You can clear IP device tracking information for AAA servers.

SUMMARY STEPS

1. (Optional) **clear ip device tracking all**
2. (Optional) **clear ip device tracking interface ethernet** *slot*/*port*
3. (Optional) **clear ip device tracking ip-address** *ipv4-address*
4. (Optional) **clear ip device tracking mac-address** *mac-address*
5. (Optional) **show ip device tracking all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **clear ip device tracking all** **Example:** `switch# clear ip device tracking all`	Clears all EAPoUDP sessions.
Step 2	(Optional) **clear ip device tracking interface ethernet** *slot*/*port* **Example:** `switch# clear ip device tracking interface ethernet 2/1`	Clears EAPoUDP sessions on a specified interface.
Step 3	(Optional) **clear ip device tracking ip-address** *ipv4-address* **Example:** `switch# clear ip device tracking ip-address 10.10.1.1`	Clears an EAPoUDP session for a specified IPv4 address in the format A.B.C.D.
Step 4	(Optional) **clear ip device tracking mac-address** *mac-address* **Example:** `switch# clear ip device tracking mac-address 000c.30da.86f4`	Clears an EAPoUDP session for a specified MAC address in the format XXXX.XXXX.XXXX.
Step 5	(Optional) **show ip device tracking all** **Example:** `switch# show ip device tracking all`	Displays IP device tracking information.

Manually Initializing EAPoUDP Sessions

You can manually initialize EAPoUDP sessions.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. (Optional) **eou initialize all**

2. (Optional) **eou initialize authentication** {**clientless** | **eap** | **static**}
3. (Optional) **eou initialize interface ethernet** *slot*/*port*
4. (Optional) **eou initialize ip-address** *ipv4-address*
5. (Optional) **eou initialize mac-address** *mac-address*
6. (Optional) **eou initialize posturetoken** *name*
7. (Optional) **show eou all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **eou initialize all** **Example:** `switch# eou initialize all`	Initializes all EAPoUDP sessions.
Step 2	(Optional) **eou initialize authentication** {**clientless** | **eap** | **static**} **Example:** `switch# eou initialize authentication static`	Initializes EAPoUDP sessions with a specified authentication type.
Step 3	(Optional) **eou initialize interface ethernet** *slot*/*port* **Example:** `switch# eou initialize interface ethernet 2/1`	Initializes EAPoUDP sessions on a specified interface.
Step 4	(Optional) **eou initialize ip-address** *ipv4-address* **Example:** `switch# eou initialize ip-address 10.10.1.1`	Initializes an EAPoUDP session for a specified IPv4 address in the format A.B.C.D.
Step 5	(Optional) **eou initialize mac-address** *mac-address* **Example:** `switch# eou initialize mac-address 000c.30da.86f4`	Initializes an EAPoUDP session for a specified MAC address in the format XXXX.XXXX.XXXX.
Step 6	(Optional) **eou initialize posturetoken** *name* **Example:** `switch# eou initialize posturetoken Healthy`	Initializes an EAPoUDP session for a specific posture token name. **Note** Use the **show eou all** command to display the token names.
Step 7	(Optional) **show eou all** **Example:** `switch# show eou all`	Displays the EAPoUDP session configuration.

Related Topics

Enabling EAPoUDP, on page 310

Manually Revalidating EAPoUDP Sessions

You can manually revalidate EAPoUDP sessions.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. (Optional) **eou revalidate all**
2. (Optional) **eou revalidate authentication** {**clientless** | **eap** | **static**}
3. (Optional) **eou revalidate interface ethernet** *slot*/*port*
4. (Optional) **eou revalidate ip-address** *ipv4-address*
5. (Optional) **eou revalidate mac-address** *mac-address*
6. (Optional) **eou revalidate posturetoken** *name*
7. (Optional) **show eou all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **eou revalidate all** **Example:** `switch# eou revalidate all`	Revalidates all EAPoUDP sessions.
Step 2	(Optional) **eou revalidate authentication** {**clientless** | **eap** | **static**} **Example:** `switch# eou revalidate authentication static`	Revalidates EAPoUDP sessions with a specified authentication type.
Step 3	(Optional) **eou revalidate interface ethernet** *slot*/*port* **Example:** `switch# eou revalidate interface ethernet 2/1`	Revalidates EAPoUDP sessions on a specified interface.
Step 4	(Optional) **eou revalidate ip-address** *ipv4-address* **Example:** `switch# eou revalidate ip-address 10.10.1.1`	Revalidates an EAPoUDP session for a specified IPv4 address.
Step 5	(Optional) **eou revalidate mac-address** *mac-address* **Example:** `switch# eou revalidate mac-address 000c.30da.86f4`	Revalidates an EAPoUDP session for a specified MAC address.
Step 6	(Optional) **eou revalidate posturetoken** *name* **Example:** `switch# eou revalidate posturetoken Healthy`	Revalidates an EAPoUDP session for a specific posture token name. **Note** Use the **show eou all** command to display the token names.

	Command or Action	Purpose
Step 7	(Optional) **show eou all** **Example:** `switch# show eou all`	Displays the EAPoUDP session configuration.

Related Topics

Enabling EAPoUDP, on page 310

Clearing EAPoUDP Sessions

You can clear EAPoUDP sessions from the Cisco NX-OS device.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. (Optional) **clear eou all**
2. (Optional) **clear eou authentication** {**clientless** | **eap** | **static**}
3. (Optional) **clear eou interface ethernet** *slot/port*
4. (Optional) **clear eou ip-address** *ipv4-address*
5. (Optional) **clear eou mac-address** *mac-address*
6. (Optional) **clear eou posturetoken** *name*
7. (Optional) **show eou all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **clear eou all** **Example:** `switch# clear eou all`	Clears all EAPoUDP sessions.
Step 2	(Optional) **clear eou authentication** {**clientless** | **eap** | **static**} **Example:** `switch# clear eou authentication static`	Clears EAPoUDP sessions with a specified authentication type.
Step 3	(Optional) **clear eou interface ethernet** *slot/port* **Example:** `switch# clear eou interface ethernet 2/1`	Clears EAPoUDP sessions on a specified interface.
Step 4	(Optional) **clear eou ip-address** *ipv4-address* **Example:** `switch# clear eou ip-address 10.10.1.1`	Clears an EAPoUDP session for a specified IPv4 address.

	Command or Action	Purpose
Step 5	(Optional) **clear eou mac-address** *mac-address* **Example:** `switch# clear eou mac-address 000c.30da.86f4`	Clears an EAPoUDP session for a specified MAC address.
Step 6	(Optional) **clear eou posturetoken** *name* **Example:** `switch# clear eou posturetoken Healthy`	Clears an EAPoUDP session for a specific posture token name. **Note** Use the **show eou all** command to display the token names.
Step 7	(Optional) **show eou all** **Example:** `switch# show eou all`	Displays the EAPoUDP session configuration.

Related Topics

Enabling EAPoUDP, on page 310

Disabling the EAPoUDP Feature

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

⚠ **Caution** Disabling EAPoUDP removes all EAPoUDP configuration from the Cisco NX-OS device.

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. **no feature eou**
3. **exit**
4. (Optional) **show feature**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no feature eou**	Disables EAPoUDP.

	Command or Action	Purpose
	Example: `switch(config)# no feature eou`	**Caution** Disabling the EAPoUDP feature removes all EAPoUDP configuration.

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

Step 4	(Optional) **show feature** **Example:** `switch# show feature`	Displays the enabled or disabled status for the Cisco NX-OS features.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the NAC Configuration

To display NAC configuration information, perform one of the following tasks:

Command	Purpose
show eou [**all** | **authentication** {**clientless** | **eap** | **static**} | **interface ethernet** *slot/port* | **ip-address** *ipv4-address* | **mac-address** *mac-address* | **posturetoken** *name*]	Displays the EAPoUDP configuration.
show ip device tracking [**all** | **interface ethernet** *slot/port* | **ip-address** *ipv4-address* | **mac-address** *mac-address*]	Displays IP device tracking information.
show running-config eou [**all**]	Displays the EAPoUDP configuration in the running configuration.
show startup-config eou	Displays the EAPoUDP configuration in the startup configuration.

For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuration Example for NAC

The following example shows how to configure NAC:

```
feature eou
aaa authentication eou default group radius
mac access-list macacl-01
  10 permit any any 0x100
```

```
interface Ethernet8/1
  mac access-group macacl-01
```

Additional References for NAC

This section lists the additional references for NAC.

Related Documents

Related Topic	Document Title
Cisco NX-OS licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

CHAPTER 13

Configuring Cisco TrustSec

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

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Cisco TrustSec

This section provides information about Cisco TrustSec.

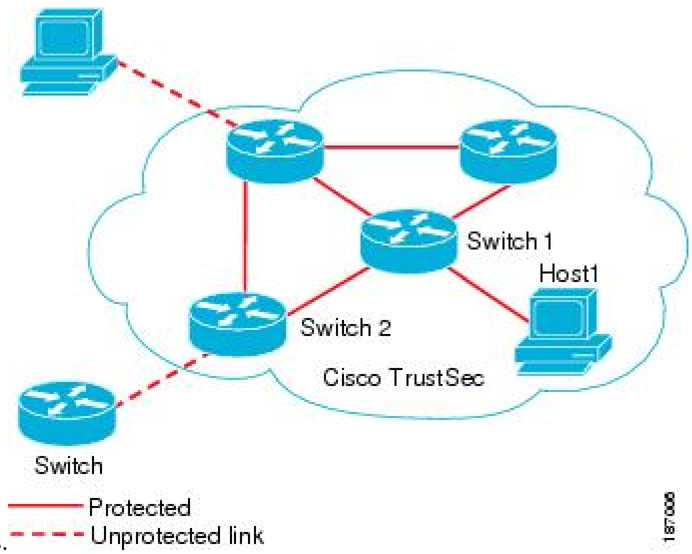
Cisco TrustSec Architecture

The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices. Each device in a cloud is authenticated by its neighbors. Communication on the links between devices in the cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms. Cisco TrustSec uses the device and user identification 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.

Figure 12: Cisco TrustSec Network Cloud Example

This figure shows an example of a Cisco TrustSec network cloud. In this example, several networking devices and an endpoint device are inside the cloud. One endpoint device and one networking device are outside the cloud because they are not Cisco TrustSec-capable devices or they have been refused



access.

The Cisco TrustSec architecture consists of the following major components:

Authentication
: Verifies the identity of each device before allowing it to join the Cisco TrustSec network

Authorization
: Decides the level of access to the Cisco TrustSec network resources for a device based on its authenticated identity

Access Control
: Applies access policies on a per-packet basis using the source tags on each packet

Secure communication
: Provides encryption, integrity, and data-path replay protection for the packets that flow over each link in the Cisco TrustSec network

A Cisco TrustSec network has the following entities:

Supplicants
: Devices that attempt to join a Cisco TrustSec network

Authenticators (AT)
: Devices that are already part of a Cisco TrustSec network

Authorization Server
Servers that might provide authentication information, authorization information, or both

When the link between the supplicant and the AT comes up, the following sequence of events might occur:

Authentication (802.1X)
The authentication server authenticates the supplicant or the authentication is completed if you configure the devices to unconditionally authenticate each other.

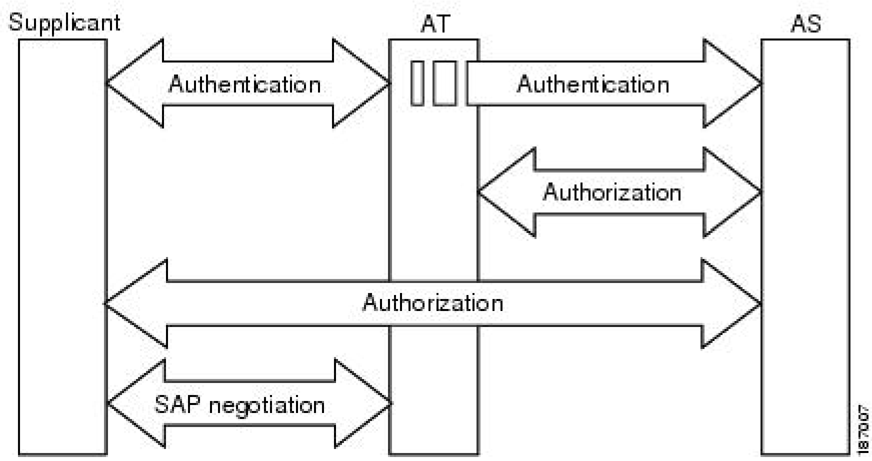
Authorization
Each side of the link obtains policies, such as SGT and ACLs, that apply to the link. A supplicant might need to use the AT as a relay if it has no other Layer 3 route to the authentication server.

Security Association Protocol Negotiation
The EAPOL-Key exchange occurs between the supplicant and the AT to negotiate a cipher suite, exchange security parameter indexes (SPIs), and manage keys. Successful completion of all three tasks results in the establishment of a security association (SA).

The ports stay in the unauthorized state (blocking state) until the SA protocol negotiation is complete.

Figure 13: SA Protocol Negotiation

This figure shows the SA protocol negotiation, including how the ports stay in unauthorized state until the SA protocol negotiation is



complete.

SA protocol negotiation can use any of the following modes of operation:

- Galois/Counter Mode (GCM) encryption
- GCM authentication (GMAC)
- No encapsulation (clear text)
- Encapsulation with no encryption or authentication

Based on the IEEE 802.1AE standard, Cisco TrustSec uses ESP-128 GCM and GMAC.

Authentication

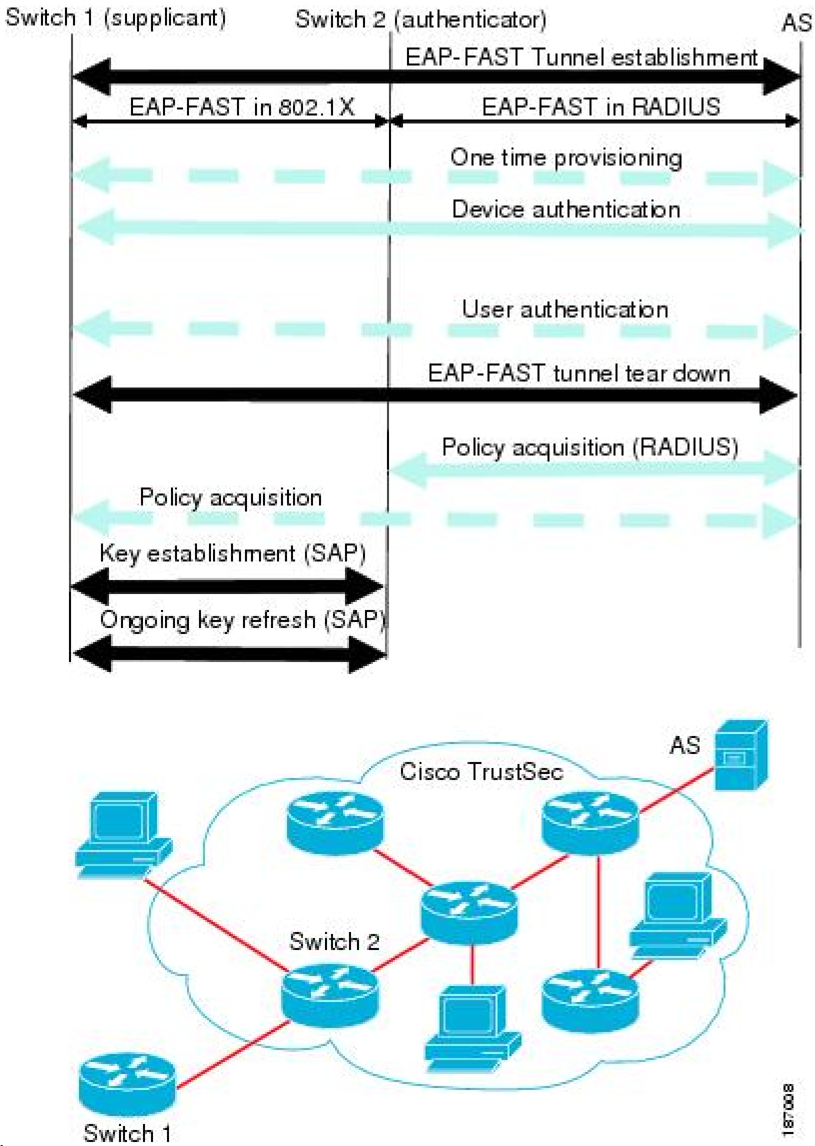
Cisco TrustSec authenticates a device before allowing it to join the network. Cisco TrustSec uses 802.1X authentication with Extensible Authentication Protocol Flexible Authentication through Secure Tunnel (EAP-FAST) as the Extensible Authentication Protocol (EAP) method to perform the authentication.

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, such as Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2), while still having security provided by the EAP-FAST tunnel.

Figure 14: Cisco TrustSec Authentication

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



TrustSec.

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.

Figure 15: SGACL Policy Example

This figure shows an example of an SGACL policy.

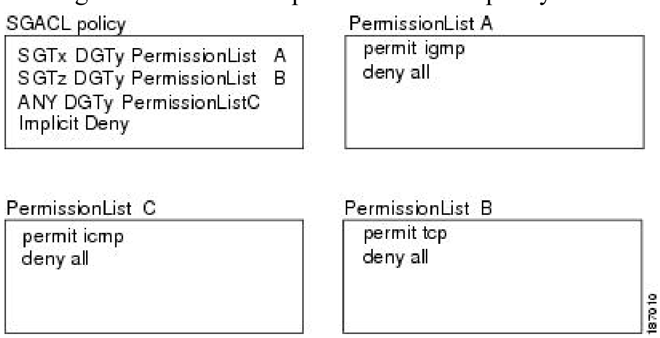
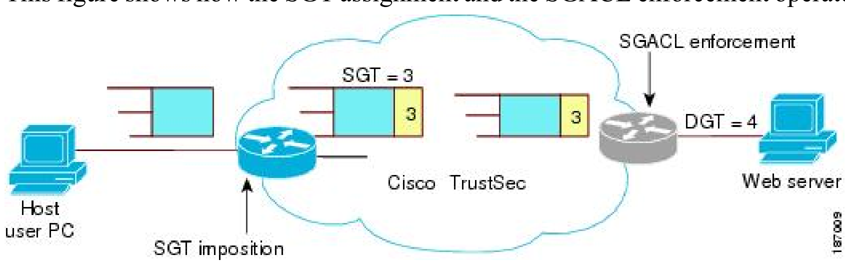


Figure 16: SGT and SGACL in Cisco TrustSec Network

This figure shows how the SGT assignment and the SGACL enforcement operate in a Cisco TrustSec network.



The Cisco NX-OS device defines the Cisco TrustSec access control policy for a group of devices as opposed to IP addresses in traditional ACLs. With such a decoupling, the network devices are free to move throughout the network and change IP addresses. Entire network topologies can change. As long as the roles and the permissions remain the same, changes to the network do not change the security policy. This feature greatly reduces the size of ACLs and simplifies their maintenance.

In traditional IP networks, the number of access control entries (ACEs) configured is determined as follows:

Number of ACEs = (number of sources specified) X (number of destinations specified) X (number of permissions specified)

Cisco TrustSec uses the following formula:

Number of ACEs = number of permissions specified

For information about SGACL policy enforcement with SGT caching, see SGACL Policy Enforcement With Cisco TrustSec SGT Caching.

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:

```
cts 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
```

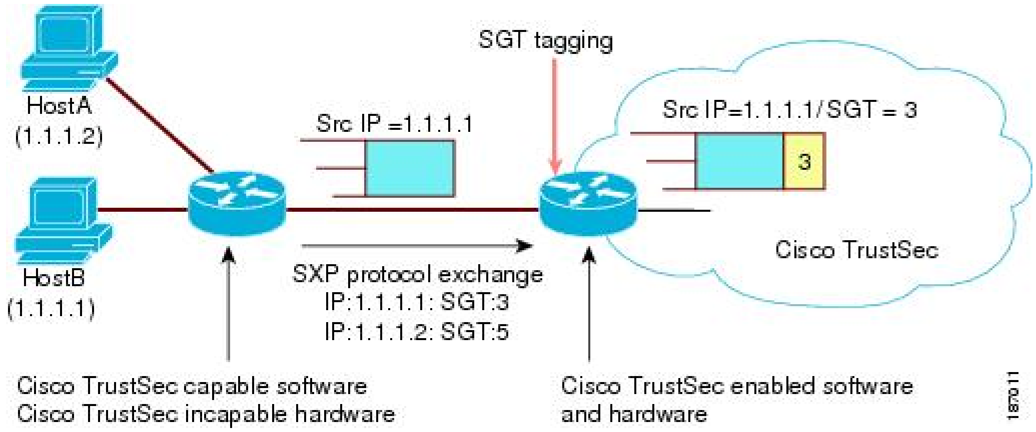
SXP for SGT Propagation Across Legacy Access Networks

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 17: 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.

Tip 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.

Note 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.

Virtualization Support

Cisco TrustSec configuration and operation are local to the virtual device context (VDC). For more information on VDCs, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide.

Licensing Requirements for Cisco TrustSec

The following table shows the licensing requirements for this feature:

Table 23: Licensing Requirements for Cisco TrustSec

Product	License Requirement
Cisco NX-OS	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. **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 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

- MACSec functionality on vPC/vPC+ members is supported on F2e series modules from Cisco NX-OS Release 6.2(10) and on F3 series modules from Cisco NX-OS Release 7.2(0)D1(1).
- Cisco TrustSec (including MACsec) is not supported over a virtual port channel (vPC) or vPC+ prior to Cisco NX-OS Release 6.2(10).
- F1 Series modules do not support Cisco TrustSec.
- The following commands are not supported for F1 Series modules:
  - cts dot1x
  - replay-protection
  - sap pmk

    - sap hash-algorithm

- CTS SGACL is supported for the F2 series and F2e series modules.
- The F2 series modules do not support the cts-dot1x mode or the cts-manual mode.
- The F1 series modules do not support FIPS mode.
- Cisco TrustSec uses RADIUS for authentication.
- 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).
- Cisco TrustSec supports IPv4 addressing only.
- 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.
- When a switch is in N-Port Virtualization (NPV) mode, an Ethernet interface that is bound to a virtual Fibre Channel in NP mode cannot be assigned a valid SGT. This restriction ensures that SGT and DGT label lookups fail so that the role-based access control list (RBACL) label configured on the logical interface is used for egress Layer 3 binding checks.
- The 40G and 100G M2 Series modules support IEEE 802.1AE MAC security (MACsec). For MACsec links that have a bandwidth that is greater than or equal to 40G, multiple security associations (SCI/AN pairs) are established with each Security Association Protocol (SAP) exchange. The F1 Series modules do not support MACsec.
- Cisco Nexus 7000 Series Switches has the debounce timer feature to delay the notification of link change, which can decrease traffic loss due to network reconfiguration. This feature affects the CTS Macsec and if delays on links are higher, the MACsec-enabled links may not come up. To bring the link up, increase the value of debounce timer link down from its default value 100. For more information about debounce timer, see the Configuring the Debounce Timer section in the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*.

Default Settings for Cisco TrustSec Parameters

This table lists the default settings for Cisco TrustSec parameters.

Table 24: Default Cisco TrustSec Parameters Settings

Parameter	Default
Cisco TrustSec	Disabled

Parameter	Default
Encryption and decryption of pause frames on all interfaces	Enabled on line cards that support the encryption and decryption of pause frames
SXP	Disabled
SXP default password	None
SXP reconcile period	120 seconds (2 minutes)
SXP retry period	60 seconds (1 minute)
Caching	Disabled
RBACL logging	Disabled
RBACL statistics	Disabled

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.

SUMMARY STEPS

1. **configure terminal**
2. **feature dot1x**
3. **feature cts**
4. **exit**
5. (Optional) **show cts**
6. (Optional) **show feature**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
Step 2	**feature dot1x** **Example:** `switch(config)# feature dot1x`	Enables the 802.1X feature.
Step 3	**feature cts** **Example:** `switch(config)# feature cts`	Enables the Cisco TrustSec feature.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 5	(Optional) **show cts** **Example:** `switch# show cts`	Displays the Cisco TrustSec configuration.
Step 6	(Optional) **show feature** **Example:** `switch# show feature`	Displays the enabled status for features.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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:

http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-installation-and-configuration-guides-list.html

Before you begin

Ensure that you have enabled Cisco TrustSec.

SUMMARY STEPS

1. **configure terminal**
2. **cts device-id** *name* **password** *password*
3. **exit**
4. (Optional) **show cts**
5. (Optional) **show cts environment**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**cts device-id** *name* **password** *password* **Example:** `switch(config)# cts device-id MyDevice1 password Cisco321`	Configures a unique device ID and password. The *name* argument has a maximum length of 32 characters and is case sensitive. **Note** To remove the configuration of device ID and the password, use the **no** form of the command.

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

Step 4	(Optional) **show cts** **Example:** `switch# show cts`	Displays the Cisco TrustSec configuration.
Step 5	(Optional) **show cts environment** **Example:** `switch# show cts environment`	Displays the Cisco TrustSec environment data.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353

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.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **key** [**0** | **7**] *key* **pac**
3. (Optional) **show radius-server**
4. **aaa group server radius** *group-name*
5. **server** {*ipv4-address* | *ipv6-address* | *hostname*}
6. **use-vrf** *vrf-name*
7. **exit**
8. **aaa authentication dot1x default group** *group-name*
9. **aaa authorization cts default group** *group-name*
10. **exit**
11. (Optional) **show radius-server groups** [*group-name*]
12. (Optional) **show aaa authentication**
13. (Optional) **show aaa authorization**
14. (Optional) **show cts pacs**
15. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **key** [**0** | **7**] *key* **pac** **Example:** `switch(config)# radius-server host 10.10.1.1 key L1a0K2s9 pac`	Configures a RADIUS server host with a key and PAC. The *hostname* argument is alphanumeric, case sensitive, and has a maximum of 256 characters. The *key* argument is alphanumeric, case sensitive, and has a maximum length of 63 characters. The **0** option indicates that the key is in clear text. The **7** option indicates that the key is encrypted. The default is clear text.
Step 3	(Optional) **show radius-server** **Example:** `switch# show radius-server`	Displays the RADIUS server configuration.

Step 4	**aaa group server radius** *group-name*
	Example:
	`switch(config)# aaa group server radius Rad1`
	`switch(config-radius)#`
		Specifies the RADIUS server group and enters RADIUS server group configuration mode.

Step 5	**server** {*ipv4-address* | *ipv6-address* | *hostname*} **Example:** `switch(config-radius)# server 10.10.1.1`	Specifies the RADIUS server host address.
Step 6	**use-vrf** *vrf-name* **Example:** `switch(config-radius)# use-vrf management`	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 7	**exit**
	Example:
	`switch(config-radius)# exit`
	`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.

	Command or Action	Purpose
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`
	`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.
Step 12	(Optional) **show aaa authentication** **Example:** `switch# show aaa authentication`	Displays the AAA authentication configuration.
Step 13	(Optional) **show aaa authorization** **Example:** `switch# show aaa authorization`	Displays the AAA authorization configuration.
Step 14	(Optional) **show cts pacs** **Example:** `switch# show cts pacs`	Displays the Cisco TrustSec PAC information.
Step 15	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353
Configuring AAA on Cisco TrustSec Nonseed Cisco NX-OS Devices , on page 358

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.

SUMMARY STEPS

1. **configure terminal**
2. **aaa group server radius aaa-private-sg**
3. **use-vrf** *vrf-name*
4. **exit**
5. (Optional) **show radius-server groups aaa-private-sg**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**aaa group server radius aaa-private-sg**
	Example:
	`switch(config)# aaa group server radius aaa-private-sg`
	`switch(config-radius)#`
		Specifies the RADIUS server group aaa-private-sg and enters RADIUS server group configuration mode.

Step 3	**use-vrf** *vrf-name* **Example:** `switch(config-radius)# use-vrf MyVRF`	Specifies the management VRF instance for the AAA server group.

Step 4	**exit**
	Example:
	`switch(config-radius)# exit`
	`switch(config)#`
		Exits RADIUS server group configuration mode.

Step 5	(Optional) **show radius-server groups aaa-private-sg** **Example:** `switch(config)# show radius-server groups aaa-private-sg`	Displays the RADIUS server group configuration for the default server group.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353
Configuring AAA on a Seed Cisco NX-OS Device in a Cisco TrustSec Network, on page 356

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:

Step 1 Enable the Cisco TrustSec feature. See Enabling the Cisco TrustSec SGT Feature , on page 353.

Step 2 Enable Cisco TrustSec authentication. See Enabling Cisco TrustSec Authentication , on page 360.

Step 3 Enable 802.1X authentication for Cisco TrustSec on the interfaces.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353
Enabling Cisco TrustSec Authentication , on page 360

Enabling Cisco TrustSec Authentication

You must enable Cisco TrustSec authentication on the interfaces. By default, the data path replay protection feature is enabled and the SA protocol operating mode is GCM-encrypt.

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 and SA protocol on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port* [- *port2*]
3. **cts dot1x**
4. (Optional) **no replay-protection**
5. (Optional) **sap modelist** {**gcm-encrypt** | **gcm-encrypt-256** | **gmac** | **no-encap** | **null**}
6. **exit**
7. **shutdown**
8. **no shutdown**
9. **exit**
10. (Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*}
11. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot*/*port* [**-** *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	(Optional) **sap modelist** {**gcm-encrypt** | **gcm-encrypt-256** | **gmac** | **no-encap** | **null**} **Example:** `switch(config-if-cts-dot1x)# sap modelist gcm-encrypt`	Configures the SAP operation mode on the interface. Use the **gcm-encrypt** keyword for GCM encryption. This option is the default. Use the **gcm-encrypt-256** keyword for 256-bit GCM encryption. Use the **gmac** keyword for GCM authentication only. Use the **no-encap** keyword for no encapsulation for SA protocol and no SGT insertion. Use the **null** keyword for encapsulation without authentication or encryption.

Step 6	**exit**
	Example:
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Exits Cisco TrustSec 802.1X configuration mode.

Step 7	**shutdown** **Example:** `switch(config-if)# shutdown`	Disables the interface.
Step 8	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface and enables Cisco TrustSec authentication on the interface.

	Command or Action	Purpose

Step 9	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 10	(Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*} **Example:** `switch(config)# show cts interface all`	Displays the Cisco TrustSec configuration on the interfaces.
Step 11	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353

Configuring Data-Path Replay Protection for Cisco TrustSec on Interfaces and Port Profiles

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

When this task is configured on a port profile, any port profile that joins the group inherits the configuration.

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port* [- *port2*]
3. **cts dot1x**
4. **no replay-protection**
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. (Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*}
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot*/*port* [- *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	**no replay-protection** **Example:** `switch(config-if-cts-dot1x)# no replay-protection`	Disables data-path replay protection. The default is enabled. Use the **replay-protection** command to enable data-path replay protection on the interface.

Step 5	**exit**
	Example:
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Exits Cisco TrustSec 802.1X configuration mode.

Step 6	**shutdown** **Example:** `switch(config-if)# shutdown`	Disables the interface.
Step 7	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface and disables the data-path reply protection feature on the interface.

Step 8	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 9	(Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*} **Example:** `switch(config)# show cts interface all`	Displays the Cisco TrustSec configuration on the interface.
Step 10	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

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

Related Topics

Enabling Cisco TrustSec Authentication , on page 360

Configuring SA Protocol Operation Modes for Cisco TrustSec on Interfaces and Port Profiles

You can configure the SA protocol operation mode on the interfaces for Layer 2 Cisco TrustSec. The default SA protocol operation mode is GCM-encrypt.

When this task is configured on a port profile, any port profile that joins the group inherits the configuration.

> **Caution** For the SA protocol operation 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 authentication on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port* [- *port2*]
3. **cts dot1x**
4. **sap modelist** [**gcm-encrypt** | **gcm-encrypt-256** | **gmac** | **no-encap** | **null**]
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. (Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot/port*}
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port* [- *port2*]
	Example:
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		Specifies a single interface or a range of interfaces and enters interface configuration mode.

	Command or Action	Purpose

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	**sap modelist** [**gcm-encrypt** | **gcm-encrypt-256** | **gmac** | **no-encap** | **null**] **Example:** `switch(config-if-cts-dot1x)# sap modelist gmac`	Configures the SA protocol authentication mode on the interface. Use the **gcm-encrypt** keyword for GCM encryption. This option is the default. Use the **gcm-encrypt-256** keyword for 256-bit GCM encryption. Use the **gmac** keyword for GCM authentication only. Use the **no-encap** keyword for no encapsulation for SA protocol on the interface and no SGT insertion. Use the **null** keyword for encapsulation without authentication or encryption for SA protocol on the interface. Only the SGT is encapsulated.

Step 5	**exit**
	Example:
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Exits Cisco TrustSec 802.1X configuration mode.

Step 6	**shutdown** **Example:** `switch(config-if)# shutdown`	Disables the interface.
Step 7	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface and SA protocol operation mode on the interface.

Step 8	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 9	(Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot/port*} **Example:** `switch(config)# show cts interface all`	Displays the Cisco TrustSec configuration on the interface.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling Cisco TrustSec Authentication , on page 360

Configuring SGT Propagation for Cisco TrustSec on Interfaces and Port Profiles

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.

When this task is configured on a port profile, any port profile that joins the group inherits the configuration.

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.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port* [- *port2*]
3. **cts dot1x**
4. **no propagate-sgt**
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. (Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*}
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot*/*port* [- *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:**	Enables 802.1X authentication for Cisco TrustSec and enters Cisco TrustSec 802.1X configuration mode.

	Command or Action	Purpose
	`switch(config-if)# cts dot1x` `switch(config-if-cts-dot1x)#`	
Step 4	**no propagate-sgt** **Example:** `switch(config-if-cts-dot1x)# no propagate-sgt`	Disables SGT propagation. The default is enabled. Use the **propagate-sgt** command to enable SGT propagation on the interface.

Step 5	**exit**
	Example:
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Exits Cisco TrustSec 802.1X configuration mode.

Step 6	**shutdown** **Example:** `switch(config-if)# shutdown`	Disables the interface.
Step 7	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface and disables the data-path reply protection feature on the interface.

Step 8	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 9	(Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot/port*} **Example:** `switch(config)# show cts interface all`	Displays the Cisco TrustSec configuration on the interface.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling Cisco TrustSec Authentication , on page 360

Regenerating SA Protocol Keys on an Interface

You can trigger an SA protocol exchange to generate a new set of keys and protect the data traffic flowing on an interface.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **cts rekey ethernet** *slot/port*
2. (Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot/port*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**cts rekey ethernet** *slot/port* **Example:** `switch# cts rekey ethernet 2/3`	Generates the SA protocol keys for an interface.
Step 2	(Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot/port*} **Example:** `switch# show cts interface all`	Displays the Cisco TrustSec configuration on the interfaces.

Related Topics

Enabling Cisco TrustSec Authentication , on page 360

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.

Caution 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.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface slot/port*
3. **cts manual**
4. **sap pmk** {*key* [**left-zero-padded**] [**display encrypt**] | **encrypted** *encrypted_pmk* | **use-dot1x**} [**modelist** {**gcm-encrypt** |**gcm-encrypt-256** | **gmac** | **no-encap** | **null**}]
5. (Optional) **policy dynamic identity** *peer-name*

6. (Optional) **policy static sgt** *tag* [**trusted**]
7. **exit**
8. **shutdown**
9. **no shutdown**
10. **exit**
11. (Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*}
12. (Optional) **show cts sap pmk** {**all** | **interface ethernet** *slot*/*port*}
13. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

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

Step 3	**cts manual**
	Example:
	`switch(config-if)# cts manual`
	`switch(config-if-cts-manual)#`
		Enters Cisco TrustSec manual configuration mode.
		Note You cannot enable Cisco TrustSec on interfaces in half-duplex mode.

Step 4	**sap pmk** {*key* [**left-zero-padded**] [**display encrypt**] | **encrypted** *encrypted_pmk* | **use-dot1x**} [**modelist** {**gcm-encrypt** |**gcm-encrypt-256** | **gmac** | **no-encap** | **null**}] **Example:** `switch(config-if-cts-manual)# sap pmk fedbaa modelist gmac`	Configures the SA protocol pairwise master key (PMK) and operation mode. SA protocol is disabled by default in Cisco TrustSec manual mode. The *key* argument is a hexadecimal value with an even number of characters and a maximum length of 32 characters. Use the **left-zero-padded** keyword to pad zeros to the left of the entered string if the PMK length is less than 32 bytes. Use the **display encrypt** keyword to specify that the configured PMK be displayed in AES-encrypted format in the running configuration. Use the **encrypted** *encrypted_pmk* keyword to specify an encrypted PMK string of 64 bytes (128 hexadecimal characters). Use the **use-dot1x** keyword when the peer device does not support Cisco TrustSec 802.1X authentication or authorization but does support SA protocol data path encryption and authentication.

	Command or Action	Purpose
		The mode list configures the cipher mode for the data path encryption and authentication as follows: Use the **gcm-encrypt** keyword for GCM encryption. This option is the default. Use the **gcm-encrypt-256** keyword for GCM encryption. Use the **gmac** keyword for GCM authentication. Use the **no-encap** keyword for no encapsulation and no SGT insertion. Use the **null** keyword for encapsulation of the SGT without authentication or encryption.
Step 5	(Optional) **policy dynamic identity** *peer-name* **Example:** `switch(config-if-cts-manual)# policy dynamic identity MyDevice2`	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. **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.
Step 6	(Optional) **policy static sgt** *tag* [**trusted**] **Example:** `switch(config-if-cts-manual)# policy static sgt 0x2`	Configures a static authorization policy. The *tag* argument is a decimal value or a hexadecimal value in the format **0x***hhhh*. The decimal range is from 2 to 65519, and the hexadecimal range is from 0x2 to 0xffef. The **trusted** keyword indicates that traffic coming on the interface with this SGT should not have its tag overridden. **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.

Step 7	**exit**
	Example:
	`switch(config-if-cts-manual)# exit`
	`switch(config-if)#`
		Exits Cisco TrustSec manual configuration mode.

Step 8	**shutdown** **Example:**	Disables the interface.

	Command or Action	Purpose
	`switch(config-if)# shutdown`	
Step 9	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface and enables Cisco TrustSec authentication on the interface.

Step 10	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 11	(Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*} **Example:** `switch# show cts interface all`	Displays the Cisco TrustSec configuration for the interfaces.
Step 12	(Optional) **show cts sap pmk** {**all** | **interface ethernet** *slot*/*port*} **Example:** `switch# show cts sap pmk all`	Displays the hexadecimal value of the configured PMK for all interfaces or a specific Ethernet interface.
Step 13	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353

Configuring Pause Frame Encryption or Decryption for Cisco TrustSec on Interfaces

Pause frames are MAC control frames used for Ethernet flow control. The ports on some line cards encrypt and decrypt pause frames while the ports on other line cards do not have this ability. This disparity causes interoperability issues and causes the ports to discard or ignore the pause frames.

You can determine if the pause frames are to be encrypted or clear on individual interfaces. You must configure the interfaces on both ends of the connection but can do so using either dot1x or manual mode. If two ports are connected to form a CTS link and one is clear pause capable and the other is secure (encryption or decryption) pause capable, the pause frames must be sent in the clear across the link in order for them to be correctly sent and received.

Note Beginning with Cisco NX-OS Release 6.2.2, all F Series and M1 Series modules support both secure (encrypted and decrypted) and clear pause frames. In prior releases, F1 Series modules, F2 Series modules, F2e Series modules, and the N7K-M132XP-12(L) module support only clear pause frames.

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.

Caution For the pause frame encryption or decryption 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.

Ensure that you have enabled flow control on the interface using the **flowcontrol** {**send** | **receive**} command.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **cts dot1x** or **cts manual**
4. [**no**] **encrypt pause-frame**
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. (Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*}
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

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

Step 3	**cts dot1x** or **cts manual**
	Example:
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Enters Cisco TrustSec dot1x or manual configuration mode.
		Note You cannot enable Cisco TrustSec on interfaces in half-duplex mode.

	Command or Action	Purpose
Step 4	[**no**] **encrypt pause-frame** **Example:** `switch(config-if-cts-dot1x)# no encrypt pause-frame`	Configures pause frame encryption or decryption for Cisco TrustSec on the interface. When **no encrypt pause-frame** is configured, the pause frames are sent in the clear. When **encrypt pause-frame** is configured, pause frames are sent encrypted over the CTS link.

Step 5	**exit**
	Example:
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Exits Cisco TrustSec dot1x or manual configuration mode.

Step 6	**shutdown** **Example:** `switch(config-if)# shutdown`	Disables the interface.
Step 7	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface and enables pause frame encryption or decryption for Cisco TrustSec on the interface.

Step 8	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 9	(Optional) **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*} **Example:** `switch# show cts interface all`	Displays the Cisco TrustSec configuration for the interfaces.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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:

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 Batch Programming

Perform the following task to enable batching of Security Group Access Control List (SGACL) programming.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **cts role-based policy batched-programming enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	[**no**] **cts role-based policy batched-programming enable**	Enables batching of SGACL programming-related tasks. To disable SGACL batch programming after you have explicitly enabled the feature, use the **no** form of this command.

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.

SUMMARY STEPS

1. **configure terminal**
2. **vlan** *vlan-id*
3. **cts role-based enforcement**
4. **exit**
5. (Optional) **show cts role-based enable**

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

DETAILED STEPS

	Command or Action	Purpose

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:** `switch(config-vlan)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on the VLAN. **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.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353

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.

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.

SUMMARY STEPS

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **cts role-based enforcement**
4. **exit**
5. (Optional) **show cts role-based enable**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**vrf context** *vrf-name*
	Example:
	`switch(config)# vrf context MyVrf`
	`switch(config-vrf)#`
		Specifies a VRF instance and enters VRF configuration mode.

Step 3	**cts role-based enforcement** **Example:** `switch(config-vrf)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on the VRF instance.

Step 4	**exit**
	Example:
	`switch(config-vrf)# exit`
	`switch(config)#`
		Exits VRF 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.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353

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.

SUMMARY STEPS

1. **configure terminal**
2. **cts sgt** *tag*
3. **exit**
4. (Optional) **show cts environment-data**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**cts sgt** *tag* **Example:** `switch(config)# cts sgt 0x00a2`	Configures the SGT for packets sent from the device. The *tag* argument is a decimal value or a hexadecimal value in the format **0x***hhhh*. The decimal range is from 2 to 65519, and the hexadecimal range is from 0x2 to 0xffef.

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

Step 4	(Optional) **show cts environment-data** **Example:** `switch# show cts environment-data`	Displays the Cisco TrustSec environment data information.
Step 5	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	`switch# copy running-config startup-config`	

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353

Manually Configuring Cisco TrustSec SGTs

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

Before you begin

Ensure that you have enabled Cisco TrustSec.

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Configure the SGT for packets sent from the device:

switch(config)# **cts sgt** *tag*

Note The *tag* argument is a decimal value or a hexadecimal value in the format **0x***hhhh*. The decimal range is from 2 to 65519, and the hexadecimal range is from 0x2 to 0xffef.

Step 3 Exit global configuration mode:

switch(config)# **exit**

Step 4 (Optional) Display the Cisco TrustSec environment data information:

switch# **show cts environment-data**

Step 5 (Optional) Copy the running configuration to the startup configuration:

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

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.

SUMMARY STEPS

1. **configure terminal**

2. **vlan** *vlan-id*
3. **cts role-based sgt-map** *ipv4-address tag*
4. **exit**
5. (Optional) **show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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 sgt-map** *ipv4-address tag* **Example:** `switch(config-vlan)# cts role-based sgt-map 10.10.1.1 100`	Configures SGT mapping for the SGACL policies for the VLAN.

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 sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*] **Example:** `switch(config)# show cts role-based sgt-map`	Displays the Cisco TrustSec SGACL SGT mapping 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.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353
Enabling SGACL Policy Enforcement on VLANs , on page 374
Enabling SGACL Policy Enforcement on VRF Instances, on page 375

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.

SUMMARY STEPS

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **cts role-based sgt-map** *ipv4-address tag*
4. **exit**
5. (Optional) **show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**vrf context** *vrf-name*
	Example:
	`switch(config)# vrf context accounting`
	`switch(config-vrf)#`
		Specifies a VRF instance and enters VRF configuration mode.

Step 3	**cts role-based sgt-map** *ipv4-address tag* **Example:** `switch(config-vrf)# cts role-based sgt-map 10.10.1.1 100`	Configures SGT mapping for the SGACL policies for the VLAN.

Step 4	**exit**
	Example:
	`switch(config-vrf)# exit`
	`switch(config)#`
		Exits VRF configuration mode.

	Command or Action	Purpose
Step 5	(Optional) **show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*] **Example:** `switch(config)# show cts role-based sgt-map`	Displays the Cisco TrustSec SGACL SGT mapping 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.

Configuring VLAN to SGT Mapping

You can map VLANs to SGTs. This procedure is useful for deploying Cisco TrustSec for devices that are VLAN capable but not SGT capable. A host or server can be assigned an SGT based on the assigned VLAN, and any traffic from the VLAN would be marked with the given SGT.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **configure terminal**
2. **vlan** *vlan-id*
3. **cts role-based sgt** *sgt-value*
4. **exit**
5. (Optional) **show cts role-based sgt vlan** {**all** | *vlan-id*}
6. (Optional) **show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*]
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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 sgt** *sgt-value* **Example:** `switch(config-vlan)# cts role-based sgt 3`	Maps the VLAN to an SGT. The *sgt-value* argument range is from 1 to 65519.

	Command or Action	Purpose

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 sgt vlan** {**all** | *vlan-id*} **Example:** `switch(config)# show cts role-based sgt vlan all`	Displays the configured SGT for the specified VLAN.
Step 6	(Optional) **show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*] **Example:** `switch(config)# show cts role-based sgt-map summary`	Displays the SGT mappings.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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. You can also enable role-based access control list (RBACL) logging, which allows users to monitor specific types of packets exiting the Cisco NX-OS device.

Note Before the system generates ACLLOG and RBACL syslogs, logged packets are rate limited, and flows are cached. You can view the source group tag (SGT) on the logged packets using the **show logging ip access-list cache detail** command. For details of this command, see the *Cisco Nexus 7000 Series NX-OS System Management Command Reference*.

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.

If you plan to enable RBACL logging, ensure that you have enabled RBACL policy enforcement on the VLAN and VRF instance.

If you plan to enable RBACL logging, ensure that you have set the logging level of ACLLOG syslogs to 6 and the logging level of CTS manager syslogs to 5.

If you plan to enable RBACL logging, ensure that you have set the logging level of CTS manager syslogs to 6 or less.

SUMMARY STEPS

1. **configure terminal**
2. **cts role-based access-list** *list-name*
3. (Optional) {**deny** | **permit**} **all** [**log**]
4. (Optional) {**deny** | **permit**} **icmp** [**log**]
5. (Optional) {**deny** | **permit**} **igmp** [**log**]
6. (Optional) {**deny** | **permit**} **ip** [**log**]
7. (Optional) {**deny** | **permit**} **tcp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}] [**log**]
8. {**deny** | **permit**} **udp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}] [**log**]
9. **exit**
10. **cts role-based sgt** {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **any** | **unknown**} **access-list** *list-name*
11. (Optional) **show cts role-based access-list**
12. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**cts role-based access-list** *list-name*
	Example:
	`switch(config)# cts role-based access-list MySGACL`
	`switch(config-rbacl)#`
		Specifies an SGACL and enters role-based access list configuration mode. The *list-name* argument value is alphanumeric, case sensitive, and has a maximum length of 32 characters.

Step 3	(Optional) {**deny** | **permit**} **all** [**log**] **Example:** `switch(config-rbacl)# deny all log`	Denies or permits all traffic. Optionally, you can use the **log** keyword to specify that packets matching this configuration be logged.
Step 4	(Optional) {**deny** | **permit**} **icmp** [**log**] **Example:** `switch(config-rbacl)# permit icmp`	Denies or permits Internet Control Message Protocol (ICMP) traffic. Optionally, you can use the **log** keyword to specify that packets matching this configuration be logged.
Step 5	(Optional) {**deny** | **permit**} **igmp** [**log**] **Example:** `switch(config-rbacl)# deny igmp`	Denies or permits Internet Group Management Protocol (IGMP) traffic. Optionally, you can use the **log** keyword to specify that packets matching this configuration be logged.
Step 6	(Optional) {**deny** | **permit**} **ip** [**log**] **Example:** `switch(config-rbacl)# permit ip`	Denies or permits IP traffic. Optionally, you can use the **log** keyword to specify that packets matching this configuration be logged.

	Command or Action	Purpose
Step 7	(Optional) {**deny** | **permit**} **tcp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}] [**log**] **Example:** `switch(config-rbacl)# deny tcp dst eq 100`	Denies or permits TCP traffic. The default permits all TCP traffic. The range for the *port-number*, *port-number1*, and *port-number2* arguments is from 0 to 65535. Optionally, you can use the **log** keyword to specify that packets matching this configuration be logged.
Step 8	{**deny** | **permit**} **udp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}] [**log**] **Example:** `switch(config-rbacl)# permit udp src eq 1312`	Denies or permits UDP traffic. The default permits all UDP traffic. The range for the *port-number*, *port-number1*, and *port-number2* arguments is from 0 to 65535. Optionally, you can use the **log** keyword to specify that packets matching this configuration be logged.

Step 9	**exit**
	Example:
	`switch(config-rbacl)# exit`
	`switch(config)#`
		Exits role-based access-list configuration mode.

Step 10	**cts role-based sgt** {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **any** | **unknown**} **access-list** *list-name* **Example:** `switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL`	Maps the SGT values to the SGACL. The *sgt-value* and *dgt-value* argument values range from 0 to 65520. **Note** You must create the SGACL before you can map SGTs to it.
Step 11	(Optional) **show cts role-based access-list** **Example:** `switch(config)# show cts role-based access-list`	Displays the Cisco TrustSec SGACL configuration.
Step 12	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353
Enabling SGACL Policy Enforcement on VLANs , on page 374
Enabling SGACL Policy Enforcement on VRF Instances, on page 375

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.

SUMMARY STEPS

1. **show cts role-based access-list**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show cts role-based access-list** **Example:** `switch# show cts role-based access-list`	Displays Cisco TrustSec SGACLs, both downloaded from the Cisco Secure ACS and manually configured on the Cisco NX-OS device.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353

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.

SUMMARY STEPS

1. **cts refresh role-based-policy sgt** {*sgt-value* | **any** | **unknown**}
2. (Optional) **show cts role-based policy**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**cts refresh role-based-policy sgt** {*sgt-value* | **any** | **unknown**}
	Example:
	`switch# cts refresh role-based-policy`
	Example:
	`switch# cts refresh role-based-policy sgt any`
		Refreshes the Cisco TrustSec SGACL policies from the Cisco Secure ACS.
		• **sgt**—Refreshes the egress policy for an SGT.
		• *sgt-value* —Refreshes the egress policy for a specified SGT.
		• **any**—Refreshes the egress policy for any SGT.
		• **unknown**—Refreshes the egress policy for an unknown SGT.

Step 2	(Optional) **show cts role-based policy** **Example:** `switch# show cts role-based policy`	Displays the Cisco TrustSec SGACL policies.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353

Refreshing the Environment Data

You can refresh the environment data download from the AAA server.

Before you begin

Ensure that you enabled Cisco TrustSec.

Ensure that you are using the Cisco Identity Services Engine (ISE) Release 1.0 or later releases.

SUMMARY STEPS

1. **cts refresh environment-data**
2. **show cts environment-data**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**cts refresh environment-data** **Example:** `switch# cts refresh environment-data`	Refreshes the environment data from the AAA server.
Step 2	**show cts environment-data** **Example:** `switch# show cts environment-data`	Displays the downloaded environment data pertaining to the local device. **Note** The SGT name table entries can be downloaded from the ISE.

Enabling Statistics for RBACL

You can request a count of the number of packets that match role-based access control list (RBACL) policies. These statistics are collected per source group tag (SGT) and destination group tag (DGT).

Note When you modify an RBACL policy, statistics for the previously assigned access control entry (ACE) are displayed, and the newly assigned ACE statistics are initialized to 0.

Note RBACL statistics are lost only when the Cisco NX-OS device reloads or you deliberately clear the statistics.

Before you begin

Ensure that you have enabled Cisco TrustSec.

If you plan to enable RBACL statistics, ensure that you have enabled RBACL policy enforcement on the VLAN and VRF instance.

When you enable RBACL statistics, each policy requires one entry in the hardware. If you do not have enough space remaining in the hardware, an error message appears, and you are unable to enable the statistics.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **cts role-based counters enable**
3. (Optional) **copy running-config startup-config**
4. **exit**
5. (Optional) **show cts role-based counters** [**sgt** {*sgt-value* | **any** | **unknown**}] [**dgt** {*dgt-value* | **any** | **unknown**}]
6. (Optional) **clear cts role-based counters**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **cts role-based counters enable** **Example:** `switch(config)# cts role-based counters enable`	Enables or disables RBACL statistics. The default is disabled.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 5	(Optional) **show cts role-based counters** [**sgt** {*sgt-value* | **any** | **unknown**}] [**dgt** {*dgt-value* | **any** | **unknown**}] **Example:** `switch# show cts role-based counters sgt 10 dgt 20`	Displays the configuration status of RBACL statistics and lists statistics for all RBACL policies. Optionally displays the total number of packets that match RBACL policies for a specific source group tag (SGT) or destination group tag (DGT). The *sgt-value* and *dgt-value* argument values range from 0 to 65519.
Step 6	(Optional) **clear cts role-based counters** **Example:** `switch# clear cts role-based counters`	Clears the RBACL statistics so that all counters are reset to 0.

Clearing Cisco TrustSec SGACL Policies

You can clear the Cisco TrustSec SGACL policies.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. (Optional) **show cts role-based policy**
2. **clear cts policy** {**all** | **peer** *device-name* | **sgt** *sgt-value*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **show cts role-based policy** **Example:** `switch# clear cts policy all`	Displays the Cisco TrustSec RBACL policy configuration.
Step 2	**clear cts policy** {**all** | **peer** *device-name* | **sgt** *sgt-value*} **Example:** `switch# clear cts policy all`	Clears the policies for Cisco TrustSec connection information.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353

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:

SUMMARY STEPS

1. Enable the Cisco TrustSec feature.
2. Enable SGACL policy enforcement on the VRF instance.
3. Enable Cisco TrustSec SXP.
4. Configure SXP peer connections.

DETAILED STEPS

Step 1 Enable the Cisco TrustSec feature.

Step 2 Enable SGACL policy enforcement on the VRF instance.

Step 3 Enable Cisco TrustSec SXP.

Step 4 Configure SXP peer connections.

Note You cannot use the management (mgmt 0) connection for SXP.

Related Topics

Enabling SGACL Policy Enforcement on VLANs , on page 374
Enabling SGACL Policy Enforcement on VRF Instances, on page 375
Manually Configuring IPv4-Address-to-SGACL SGT Mapping for a VLAN, on page 378
Manually Configuring SGACL Policies, on page 382
Enabling the Cisco TrustSec SGT Feature , on page 353
Enabling Cisco TrustSec SXP , on page 389
Configuring Cisco TrustSec SXP Peer Connections, on page 390

Enabling Cisco TrustSec SXP

You must enable Cisco TrustSec SXP before you can configure peer connections.

Before you begin

Ensure that you enabled Cisco TrustSec.

SUMMARY STEPS

1. **configure terminal**
2. **cts sxp enable**
3. **exit**
4. (Optional) **show cts sxp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**cts sxp enable** **Example:** `switch(config)# cts sxp enable`	Enables SXP for Cisco TrustSec.

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

Step 4	(Optional) **show cts sxp** **Example:** `switch# show cts sxp`	Displays the SXP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	`switch# copy running-config startup-config`	

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353

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.

SUMMARY STEPS

1. **configure terminal**
2. **cts sxp connection peer** *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none** | **required** *password*} **mode** {**speaker** | **listener** } [**vrf** *vrf-name*]
3. **exit**
4. (Optional) **show cts sxp connections**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**cts sxp connection peer** *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none** | **required** *password*} **mode** {**speaker** | **listener** } [**vrf** *vrf-name*] **Example:** `switch(config)# cts sxp connection peer 10.10.1.1 source 20.20.1.1 password default mode listener`	Configures the SXP address connection. 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:

	Command or Action	Purpose
		• 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	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show cts sxp connections** **Example:** `switch# show cts sxp connections`	Displays the SXP connections and their status.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353
Enabling Cisco TrustSec SXP , on page 389
Enabling SGACL Policy Enforcement on VRF Instances, on page 375

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.

SUMMARY STEPS

1. **configure terminal**

2. **cts sxp default password** *password*
3. **exit**
4. (Optional) **show cts sxp**
5. (Optional) **show running-config cts**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**cts sxp default password** *password* **Example:** `switch(config)# cts sxp default password A2Q3d4F5`	Configures the SXP default password.

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

Step 4	(Optional) **show cts sxp** **Example:** `switch# show cts sxp`	Displays the SXP configuration.
Step 5	(Optional) **show running-config cts** **Example:** `switch# show running-config cts`	Displays the SXP configuration in the running configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353
Enabling Cisco TrustSec SXP , on page 389

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.

SUMMARY STEPS

1. **configure terminal**
2. **cts sxp default source-ip** *src-ip-addr*
3. **exit**
4. (Optional) **show cts sxp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**cts sxp default source-ip** *src-ip-addr* **Example:** `switch(config)# cts sxp default source-ip 10.10.3.3`	Configures the SXP default source IPv4 address.

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

Step 4	(Optional) **show cts sxp** **Example:** `switch# show cts sxp`	Displays the SXP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353
Enabling Cisco TrustSec SXP , on page 389

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.

SUMMARY STEPS

1. **configure terminal**
2. **cts sxp reconcile-period** *seconds*
3. **exit**
4. (Optional) **show cts sxp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**cts sxp reconcile-period** *seconds* **Example:** `switch(config)# cts sxp reconcile-period 180`	Changes the SXP reconcile timer period. The default value is 120 seconds (2 minutes). The range is from 0 to 64000.

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

Step 4	(Optional) **show cts sxp** **Example:** `switch# show cts sxp`	Displays the SXP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353

Enabling Cisco TrustSec SXP , on page 389

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.

SUMMARY STEPS

1. **configure terminal**
2. **cts sxp retry-period** *seconds*
3. **exit**
4. (Optional) **show cts sxp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**cts sxp retry-period** *seconds* **Example:** `switch(config)# cts sxp retry-period 120`	Changes the SXP retry timer period. The default value is 60 seconds (1 minute). The range is from 0 to 64000.

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

Step 4	(Optional) **show cts sxp** **Example:** `switch# show cts sxp`	Displays the SXP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling the Cisco TrustSec SGT Feature , on page 353
Enabling Cisco TrustSec SXP , on page 389

Verifying the Cisco TrustSec Configuration

To display Cisco TrustSec configuration information, use one of the following commands:

Command	Purpose
show cts	Displays Cisco TrustSec information.
show cts capability interface {**all** | **ethernet** *slot*/*port*}	Displays the Cisco TrustSec capability of all interfaces or a specific Ethernet interface.
show cts authorization entries [**interface ethernet** *slot*/*port*.*subinterface*]	Displays the peer-policy data that is downloaded and stored as part of the Cisco TrustSec authorization for all interfaces or a specific Ethernet interface.
show cts credentials	Displays Cisco TrustSec credentials for EAP-FAST.
show cts environment-data	Displays Cisco TrustSec environmental data.
show cts interface {**all** | **brief** | **ethernet** *slot*/*port*}	Displays the Cisco TrustSec configuration for the interfaces.
show cts pacs	Displays Cisco TrustSec authorization information and PACs in the device key store.
show cts role-based access-list	Displays Cisco TrustSec SGACL information.
show cts role-based counters [**sgt** *sgt-value*] [**dgt** *dgt-value*]	Displays the configuration status of RBACL statistics and lists statistics for all RBACL policies. Optionally displays the total number of packets that match RBACL policies for a specific source group tag (SGT) or destination group tag (DGT).
show cts role-based enable	Displays Cisco TrustSec SGACL enforcement status.

Command	Purpose
show cts role-based policy [[**dgt** | **sgt**]{*value* | **any** | **unknown**}]	Displays Cisco TrustSec SGACL policy information for all destination security group tag (DGT) and source security group tag (SGT) pairs or for the specified DGTs or SGTs.
show cts role-based sgt-map [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name* | **cached** | **synched**]	Displays the Cisco TrustSec SGACL SGT map configuration. • **summary**—Displays a summary of the SGT mappings. • **sxp peer**—Displays the SGT map configuration for a specific SXP peer. • **vlan**—Displays the SGT map configuration for a specific VLAN. • **vrf**—Displays the SGT map configuration for a specific VRF. • **cached**—Displays SGT maps learnt via caching. • **synched**—Displays SGT maps learnt via Cisco Fabric Services synchronization.
show cts role-based sgt vlan {**all** | *vlan-id*}	Displays the configured SGT for all VLANs or a specific VLAN.
show cts server-list	Displays only the stored list of RADIUS servers available to Cisco TrustSec seed and nonseed devices.
show cts sxp [**connection** | **sgt-map**] [**vrf** *vrf-name*]	Displays Cisco TrustSec SXP information.
show running-config cts	Displays the Cisco TrustSec information in the running configuration.

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:

```
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:

```
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
    sap pmk abcdef modelist gmac
    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
```

The following example shows how to specify that the configured PMK be displayed in AES-encrypted format in the running configuration:

```
 interface ethernet 2/2
   cts manual
     sap pmk fedbaa display encrypt

show cts sap pmk interface ethernet 2/2
show running-config
```

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:

```
cts 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
  cts 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
  cts role-based enforcement
```

Example: Configuring IPv4 Address to SGACL SGT Mapping for the Default VRF Instance

The following example shows how to manually configure IPv4 address to SGACL SGT mapping for Cisco TrustSec role-based policies for the default VRF instance:

```
cts role-based sgt-map 10.1.1.1 20
```

Example: Configuring IPv4 Address to SGACL SGT Mapping for a Nondefault VRF Instance

The following example shows how to manually configure IPv4 address to SGACL SGT mapping for Cisco TrustSec role-based policies for a nondefault VRF instance:

```
vrf context test
  cts role-based sgt-map 30.1.1.1 30
```

Example: Configuring IPv4 Address to SGACL SGT Mapping for a VLAN

The following example shows how to manually configure IPv4 address to SGACL SGT mapping for Cisco TrustSec role-based policies for a VLAN:

```
vlan 10
  cts role-based sgt-map 20.1.1.1 20
```

Example: Manually Configuring Cisco TrustSec SGACLs

The following example shows how to manually configure Cisco TrustSec SGACLs:

```
cts role-based access-list abcd
  permit icmp
cts role-based sgt 10 dgt 20 access-list abcd
```

The following example shows how to enable RBACL logging:

```
cts role-based access-list RBACL1
  deny tcp src eq 1111 dest eq 2222 log
cts role-based sgt 10 dgt 20 access-list RBACL1
cts role-based sgt-map 1.1.1.1 10
cts role-based sgt-map 1.1.1.2 20
```

The above configuration generates the following ACLLOG syslog:

```
%ACLLOG-6-ACLLOG_FLOW_INTERVAL: SGT: 10, Source IP: 1.1.1.1, Destination IP: 1.1.1.2, Source
 Port: 1111, Destination Port: 2222, Source Interface: Ethernet4/1, Protocol: tcp, Hit-count
 = 2
```

Note The ACLLOG syslog does not contain the destination group tag (DGT) information of the matched RBACL policy. You can find this information by looking up the IP-SGT mapping of the destination IP address in the log message and then entering the **show cts role-based sgt-map** command.

The following example shows how to enable and display RBACL statistics:

```
cts role-based counters enable
```

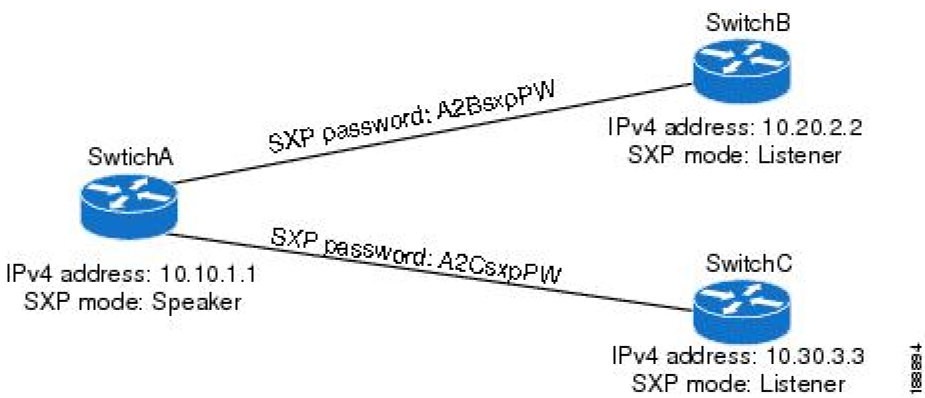
```
show cts role-based counters sgt 10 dgt 20


RBACL policy counters enabled
sgt: 10 dgt: 20 [180]
rbacl test1:
deny tcp src eq 1111 dest eq 2222   [75]
deny tcp src eq 2222 dest eq 3333   [25]
rbacl test2:
deny udp src eq 1111 dest eq 2222   [30]
deny udp src eq 2222 dest eq 3333   [50]
```

Example: Manually Configuring SXP Peer Connections

This figure shows an example of SXP peer connections over the default VRF instance.

Figure 18: Example SXP Peer Connections



The following example shows how to configure the SXP peer connections on SwitchA:

```
feature cts
cts role-based enforcement
cts sxp enable
cts sxp connection peer 10.20.2.2 password required A2BsxpPW mode listener
cts 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:

```
feature cts
cts role-based enforcement
cts sxp enable
cts 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:

```
feature cts
cts role-based enforcement
cts sxp enable
cts 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

Related Topic	Document Title
Cisco NX-OS licensing	*Cisco NX-OS Licensing Guide*
Command Reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

Feature History for Cisco TrustSec

This table lists the release history for this feature.

Table 25: Feature History for Cisco TrustSec

Feature Name	Releases	Feature Information
Cisco TrustSec	6.2(10)	Added SGT support for F3 Series modules.
Cisco TrustSec	6.2(2)	Added the ability to map VLANs to SGTs.
Cisco TrustSec	6.2(2)	Added the ability to encrypt the SAP PMK and display the PMK in encrypted format in the running configuration.
Cisco TrustSec	6.2(2)	Added the **show cts sap pmk** command to display the hexadecimal value of the configured PMK.
Cisco TrustSec	6.2(2)	Added the **show cts capability interface** command to display the Cisco TrustSec capability of interfaces.
Cisco TrustSec	6.2(2)	Enabled the **cts sgt**, **policy static sgt**, and **clear cts policy sqt** commands to accept decimal values.

Feature Name	Releases	Feature Information
Cisco TrustSec	6.2(2)	Added the ability to download sgname tables from ISE and to refresh the environment data manually and upon environment data timer expiry.
Cisco TrustSec	6.2(2)	Added optional keywords to the **show cts role-based sgt-map** command to display a summary of the SGT mappings or the SGT map configuration for a specific SXP peer, VLAN, or VRF.
Cisco TrustSec	6.2(2)	Added the **brief** keyword to the **show cts interface** command to display a brief summary for all CTS-enabled interfaces.
Cisco TrustSec	6.2(2)	Added SGT support for F2 and F2e Series modules.
Cisco TrustSec	6.1(1)	Removed the requirement for the Advanced Services license.
Cisco TrustSec	6.1(1)	Added MACsec support for 40G and 100G M2 Series modules.
Cisco TrustSec	6.0(1)	Updated for F2 Series modules.
Cisco TrustSec	5.2(1)	Supports pause frame encryption and decryption on interfaces.
SGACL policies	5.0(2)	Supports the enabling or disabling of RBACL logging.
SGACL policies	5.0(2)	Supports the enabling, disabling, monitoring, and clearing of RBACL statistics.
Cisco TrustSec	4.2(1)	No change from Release 4.1.

CHAPTER 14

Configuring IP ACLs

This chapter describes how to configure IP access control lists (ACLs) on Cisco NX-OS devices.

Unless otherwise specified, the term IP ACL refers to IPv4 and IPv6 ACLs.

Note The Cisco NX-OS release that is running on a managed device may not support all documented features or settings. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About ACLs

An 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 device determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first matching rule determines whether the packet is permitted or denied. If there is no match, the device applies the applicable implicit rule. The device 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.

ACL Types and Applications

The device supports the following types of ACLs for security traffic filtering:

FCoE ACLs
: The device applies Fibre Channel over Ethernet (FCoE) ACLs only to Fibre Channel traffic. For more information on FCoE, see the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*.

IPv4 ACLs
: The device applies IPv4 ACLs only to IPv4 traffic.

IPv6 ACLs
: The device applies IPv6 ACLs only to IPv6 traffic.

MAC ACLs
: The device applies MAC ACLs only to non-IP traffic by default; however, you can configure Layer 2 interfaces to apply MAC ACLs to all traffic.

Security-group ACLs (SGACLs)
: The device applies SGACLs to traffic tagged by Cisco TrustSec.

IP and MAC ACLs have the following types of applications:

Port ACL
: Filters Layer 2 traffic

Router ACL
: Filters Layer 3 traffic

VLAN ACL
: Filters VLAN traffic

VTY ACL
: Filters virtual teletype (VTY) traffic

This table summarizes the applications for security ACLs.

Table 26: Security ACL Applications

Application	Supported Interfaces	Types of ACLs Supported
Port ACL	• Layer 2 interfaces • Layer 2 Ethernet port-channel interfaces When a port ACL is applied to a trunk port, the ACL filters traffic on all VLANs on the trunk port.	• IPv4 ACLs • IPv6 ACLs • MAC ACLs
Router ACL	• VLAN interfaces • Physical Layer 3 interfaces • Layer 3 Ethernet subinterfaces • Layer 3 Ethernet port-channel interfaces • Layer 3 Ethernet port-channel subinterfaces • Tunnels • Management interfaces **Note** You must enable VLAN interfaces globally before you can configure a VLAN interface. For more information, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*.	• IPv4 ACLs • IPv6 ACLs **Note** MAC ACLs are supported on Layer 3 interfaces only if you enable MAC packet classification.
VLAN ACL	• VLANs	• IPv4 ACLs • IPv6 ACLs • MAC ACLs
VTY ACL	• VTYs	• IPv4 ACLs • IPv6 ACLs

Related Topics

MAC Packet Classification, on page 462
Information About MAC ACLs, on page 461
Information About VLAN ACLs, on page 473
SGACLs and SGTs , on page 346

Order of ACL Application

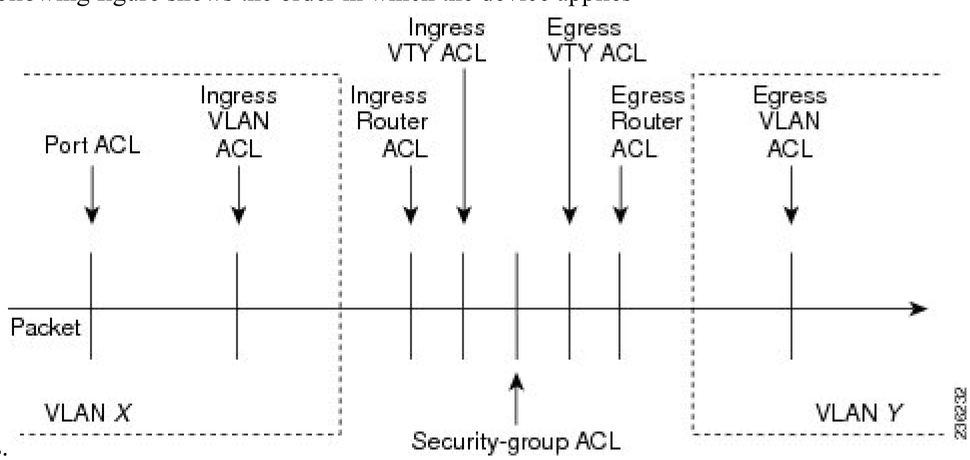
When the device processes a packet, it determines the forwarding path of the packet. The path determines which ACLs that the device applies to the traffic. The device applies the ACLs in the following order:

1. Port ACL
2. Ingress VACL
3. Ingress router ACL
4. Ingress VTY ACL
5. SGACL
6. Egress VTY ACL
7. Egress router ACL
8. Egress VACL

If the packet is bridged within the ingress VLAN, the device does not apply router ACLs.

Figure 19: Order of ACL Application

The following figure shows the order in which the device applies

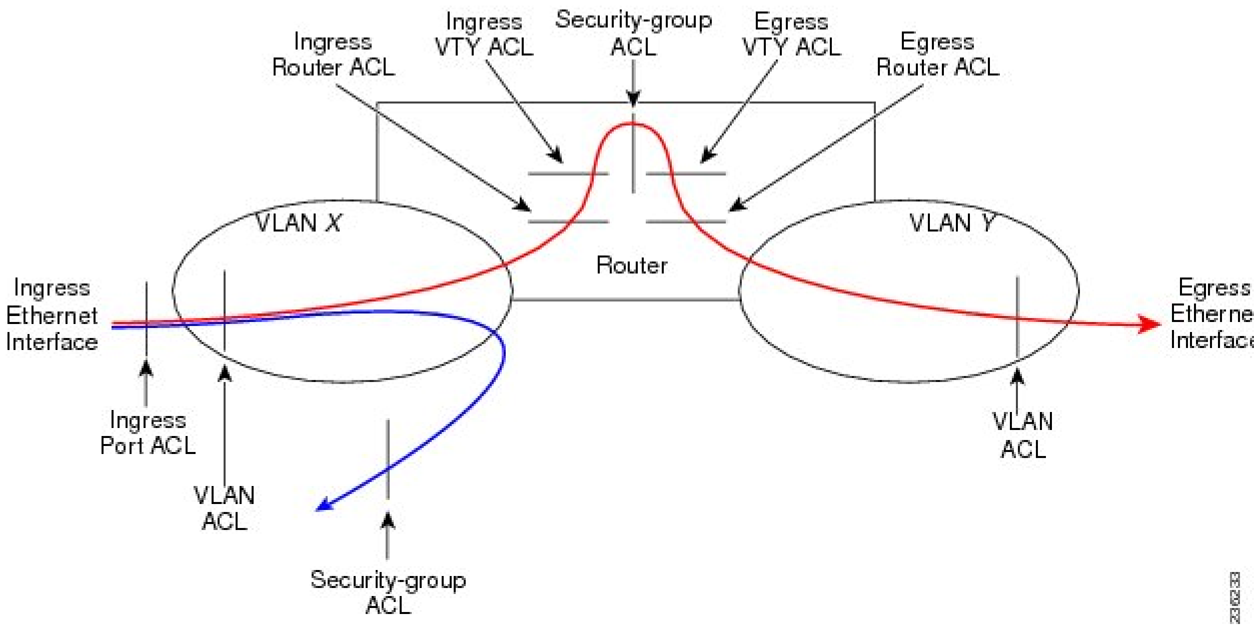


ACLs.

Figure 20: ACLs and Packet Flow

The following figure shows where the device applies ACLs, depending upon the type of ACL. The red path indicates a packet sent to a destination on a different interface than its source. The blue path indicates a packet that is bridged within its VLAN.

The device applies only the applicable ACLs. For example, if the ingress port is a Layer 2 port and the traffic is on a VLAN that is a VLAN interface, a port ACL and a router ACL both can apply. In addition, if a VACL is applied to the VLAN, the device applies that ACL too.



Related Topics

SGACLs and SGTs , on page 346

About 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.

You can create rules in access-list configuration mode by using the **permit** or **deny** command. 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. For information about every option, see the applicable **permit** and **deny** commands in the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Protocols for IP ACLs

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 or IPv6 ACL, you can specify ICMP by name.

You can specify any protocol by number. In MAC ACLs, you can specify protocols by the EtherType number of the protocol, which is a hexadecimal number. For example, you can use 0x0800 to specify IP traffic in a MAC ACL rule.

In IPv4 and IPv6 ACLs, you can specify protocols by the integer that represents the Internet protocol number. For example, you can use 115 to specify Layer 2 Tunneling Protocol (L2TP) traffic.

For a list of the protocols that each type of ACL supports by name, see the applicable **permit** and **deny** commands in the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

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. How you specify the source and destination depends on whether you are configuring IPv4, IPv6, or MAC ACLs. For information about specifying the source and destination, see the applicable **permit** and **deny** commands in the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Implicit Rules for IP and MAC ACLs

IP and MAC ACLs have implicit rules, which means that although these rules do not appear in the running configuration, the device applies them to traffic when no other rules in an ACL match. When you configure the device to maintain per-rule statistics for an ACL, the device does not maintain statistics for implicit rules.

All IPv4 ACLs include the following implicit rule:

```
deny ip any any
```

This implicit rule ensures that the device denies unmatched IP traffic.

All IPv6 ACLs include the following implicit rules:

```
permit icmp any any nd-na
permit icmp any any nd-ns
permit icmp any any router-advertisement
permit icmp any any router-solicitation
deny ipv6 any any
```

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 IPv6 ACL 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. These options differ by ACL type. The following list includes most but not all additional filtering options:

- IPv4 ACLs support the following additional filtering options:

  - Layer 4 protocol
  - Authentication Header Protocol
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Encapsulating Security Payload
  - General Routing Encapsulation (GRE)
  - KA9Q NOS-compatible IP-over-IP tunneling
  - Open Shortest Path First (OSPF)
  - Payload Compression Protocol
  - Protocol-independent multicast (PIM)
  - 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
  - Packet length

- IPv6 ACLs support the following additional filtering options:
  - Layer 4 protocol
  - Authentication Header Protocol
  - Encapsulating Security Payload
  - Payload Compression Protocol
  - Stream Control Transmission Protocol (SCTP)
  - SCTP, TCP, and UDP ports
  - ICMP types and codes
  - IGMP types
  - Flow label
  - DSCP value
  - TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
  - Established TCP connections
  - Packet length

- MAC ACLs support the following additional filtering options:
    - Layer 3 protocol
    - VLAN ID
    - Class of Service (CoS)

For information about all filtering options available in rules, see the applicable **permit** and **deny** commands in the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Sequence Numbers

The 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, Cisco NX-OS allows you to reassign sequence numbers to rules in an ACL. Resequencing 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 device stores operator-operand couples in registers called logical operator units (LOUs). Cisco Nexus 7000 Series devices support 104 LOUs.

The LOU usage for each type of operator is as follows:

eq
: Is never stored in an LOU

gt
: Uses 1/2 LOU

lt
: Uses 1/2 LOU

neq
: Uses 1/2 LOU

range
: Uses 1 LOU

The following guidelines determine when the devices store 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.

Logging

You can enable the device to create an informational log message for packets that match a rule. The log message contains the following information about the packet:

- Protocol
- Status of whether the packet is a TCP, UDP, or ICMP packet, or if the packet is only a numbered packet.
- Source and destination address
- Source and destination port numbers, if applicable

Access Lists with Fragment Control

As non-initial fragments contain only Layer 3 information, these access-list entries containing only Layer 3 information, can now be applied to non-initial fragments also. The fragment has all the information the system requires to filter, so the access-list entry is applied to the fragments of a packet.

This feature adds the optional **fragments** keyword to the following IP access list commands: **deny (IPv4)**, **permit (IPv4)**, **deny (IPv6)**, **permit (IPv6)**. By specifying the **fragments** keyword in an access-list entry, that particular access-list entry applies only to non-initial fragments of packets; the fragment is either permitted or denied accordingly.

The behavior of access-list entries regarding the presence or absence of the **fragments** keyword can be summarized as follows:

<table>
<tr><th>If the Access-List Entry has...</th><th>Then...</th></tr>
<tr><td>...no fragments keyword and all of the access-list entry information matches</td><td>For an access-list entry containing only Layer 3 information:
The entry is applied to non-fragmented packets, initial fragments, and non-initial fragments.
For an access-list entry containing Layer 3 and Layer 4 information:
The entry is applied to non-fragmented packets and initial fragments.
If the entry matches and is a permit statement, the packet or fragment is permitted.
If the entry matches and is a deny statement, the packet or fragment is denied.
The entry is also applied to non-initial fragments in the following manner. Because non-initial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and
If the entry is a permit statement, the non-initial fragment is permitted.
If the entry is a deny statement, the next access-list entry is processed.
Note The deny statements are handled differently for non-initial fragments versus non-fragmented or initial fragments.</td></tr>
<tr><td>...the fragments keyword and all of the access-list entry information matches</td><td>The access-list entry is applied only to non-initial fragments.
Note The fragments keyword cannot be configured for an access-list entry that contains any Layer 4 information.</td></tr>
</table>

You should not add the **fragments** keyword to every access-list entry, because the first fragment of the IP packet is considered a non-fragment and is treated independently of the subsequent fragments. Because an initial fragment will not match an access list permit or deny entry that contains the **fragments** keyword, the packet is compared to the next access list entry until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every deny entry. The first deny entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second deny entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple deny access list entries for the same host but with different Layer 4 ports, a single deny access-list entry with the **fragments** keyword for that host is all that has to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each fragment counts individually as a packet in access-list accounting and access-list violation counts.

Note The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

Note Within the scope of ACL processing, Layer 3 information refers to fields located within the IPv4 header; for example, source, destination, protocol. Layer 4 information refers to other data contained beyond the IPv4 header; for example, source and destination ports for TCP or UDP, flags for TCP, type and code for ICMP.

Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list had entries that match on Layer 4 through Layer 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access-list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

Note Filtering with L3 and L4 information can lead to routing or packet loss issues in the network. Perform any one of the following to prevent these issues:

- Modify the route map to allow required L3 information for appropriate UDP ports.
- Check the MTU by verifying the path from source to destination to ensure that the packet is not fragmented.

ACL Capture

You can configure ACL capture in order to selectively monitor traffic on an interface or VLAN.

When you enable the capture option for an ACL rule, packets that match this rule are either forwarded or dropped based on the specified **permit** or **deny** action and may also be copied to an alternate destination port for further analysis.

An ACL rule with the capture option can be applied as follows:

- On a VLAN
- In the ingress direction on all interfaces
- In the egress direction on all Layer 3 interfaces

ACL capture can be used in a variety of scenarios. For example, ACL capture can use ACL rules to identify packets belonging to a tunnel and to send a copy (or capture) of the tunnel packets to a specific destination. ACL capture can also be used to monitor all HTTP traffic on a particular VLAN.

Finally, you can also configure the capture session for the whole ACL rather than configuring it per ACL rule. This configuration applies the capture session to all of the ACL rules.

Related Topics

Enabling or Disabling ACL Capture, on page 436
Configuring an ACL Capture Session, on page 437
Applying an ACL with Capture Session ACEs to an Interface, on page 438
Applying a Whole ACL Capture Session to an Interface, on page 439

Time Ranges

You can use time ranges to control when an ACL rule is in effect. For example, if the device determines that a particular ACL applies to traffic arriving on an interface, and a rule in the ACL uses a time range that is not in effect, the device does not compare the traffic to that rule. The device evaluates time ranges based on its clock.

When you apply an ACL that uses time ranges, the device updates the affected I/O module whenever a time range referenced in the ACL starts or ends. Updates that are initiated by time ranges occur on a best-effort priority. If the device is especially busy when a time range causes an update, the device may delay the update by up to a few seconds.

IPv4, IPv6, and MAC ACLs support time ranges. When the device applies an ACL to traffic, the rules in effect are as follows:

- All rules without a time range specified
- Rules with a time range that includes the second when the device applies the ACL to traffic

The device supports named, reusable time ranges, which allows you to configure a time range once and specify it by name when you configure many ACL rules. Time range names have a maximum length of 64 alphanumeric characters. From Cisco NX-OS Release 8.4(2), the ACL time range name has a maximum length of 256 characters.

A time range contains one or more rules. The two types of rules are as follows:

Absolute

A rule with a specific start date and time, specific end date and time, both, or neither. The following items describe how the presence or absence of a start or end date and time affect whether an absolute time range rule is active:

- Start and end date and time both specified—The time range rule is active when the current time is later than the start date and time and earlier than the end date and time.
- Start date and time specified with no end date and time—The time range rule is active when the current time is later than the start date and time.
- No start date and time with end date and time specified—The time range rule is active when the current time is earlier than the end date and time.
- No start or end date and time specified—The time range rule is always active.

For example, you could prepare your network to allow access to a new subnet by specifying a time range that allows access beginning at midnight of the day that you plan to place the subnet online. You can use that time range in ACL rules that apply to the subnet. After the start time and date have passed, the device automatically begins applying the rules that use this time range when it applies the ACLs that contain the rules.

Periodic

A rule that is active one or more times per week. For example, you could use a periodic time range to allow access to a lab subnet only during work hours on weekdays. The device automatically applies ACL rules that use this time range only when the range is active and when it applies the ACLs that contain the rules.

Note The order of rules in a time range does not affect how a device evaluates whether a time range is active. Cisco NX-OS includes sequence numbers in time ranges to make editing the time range easier.

Time ranges also allow you to include remarks, which you can use to insert comments into a time range. Remarks have a maximum length of 100 alphanumeric characters.

The device determines whether a time range is active as follows:

- The time range contains one or more absolute rules—The time range is active if the current time is within one or more absolute rules.
- The time range contains one or more periodic rules—The time range is active if the current time is within one or more periodic rules.
- The time range contains both absolute and periodic rules—The time range is active if the current time is within one or more absolute rules and within one or more periodic rules.

When a time range contains both absolute and periodic rules, the periodic rules can only be active when at least one absolute rule is active.

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.

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.

Related Topics

Monitoring and Clearing IP ACL Statistics, on page 446
Implicit Rules for IP and MAC ACLs, on page 410

Atomic ACL Updates

An atomic ACL update is a hardware operation where both the existing ACL and the updated ACL are programmed in TCAM memory. This is the default mode of operation. The benefit of this update method is that ACL changes are not service impacting. When you make a change to the ACL, the current ACL is already programmed in TCAM. The Cisco Nexus 7000 Series device will then take the current ACL and merge it with the changes to produce ACL prime. ACL prime will also be programmed into TCAM. The Cisco Nexus 7000 Series device will then change the pointer so that ACL prime is associated with the interface. The final step is to delete the old ACL from TCAM. Functionally this means that you can never exceed 50 percent of ACL TCAM resources if you want to use atomic ACL updates. If you exceed 50 percent of ACL resources while atomic ACL update is active, the “ERROR: Tcam will be over used, please turn off atomic update” message is received and the new ACL changes are not applied.

Nonatomic ACL updates are required if you are using more than 50 percent of the ACL TCAM. When this mode is active, the Cisco Nexus 7000 Series device will remove the old ACL from TCAM and replace it with ACL prime as quickly as possible. This allows you to use up to 100 percent of your ACL TCAM but has the disadvantage that it will cause a temporary interruption in service because packets that were permitted by the old ACL will be dropped until ACL prime can be successfully programed into the ACL TCAM.

By default, when a supervisor module of a Cisco Nexus 7000 Series device updates an I/O module with changes to an ACL, it performs an atomic ACL update. An atomic update does not disrupt traffic that the updated ACL applies to; however, an atomic update requires that an I/O module that receives an ACL update has enough available resources to store each updated ACL entry in addition to all pre-existing entries in the affected ACL. After the update occurs, the additional resources used for the update are freed. If the I/O module lacks the required resources, the device generates an error message and the ACL update to the I/O module fails.

If an I/O module lacks the resources required for an atomic update, you can disable atomic updates by using the **no hardware access-list update atomic** command; however, during the brief time required for the device to remove the preexisting ACL and implement the updated ACL, traffic that the ACL applies to is dropped by default.

If you want to permit all traffic that an ACL applies to while it receives a nonatomic update, use the **hardware access-list update default-result permit** command.

Note The **hardware access-list update** command is available in the default VDC only but applies to all VDCs.

This example shows how to disable atomic updates to ACLs:

```
switch# config t
switch(config)# no hardware access-list update atomic
```

This example shows how to permit affected traffic during a nonatomic ACL update:

```
switch# config t
switch(config)# hardware access-list update default-result permit
```

This example shows how to revert to the atomic update method:

```
switch# config t
switch(config)# no hardware access-list update default-result permit
switch(config)# hardware access-list update atomic
```

Planning for Atomic ACL Updates

To adequately plan for Atomic ACL updates you need to be aware of how many ACE (Access Control Elements) you are using on all of your ACLs on each module. You also need to know how many ACEs your TCAM can support. You can find out your current usage with the **show hardware access-list resource utilization mod** *module-number* command.

```
show hardware access-list resource
utilization mod 3
 INSTANCE 0x0
 -------------
 ACL Hardware Resource Utilization (Mod 3)
 --------------------------------------------
                Used  Free  Percent
```

```
                              Utilization
-----------------------------------------------------
Tcam 0, Bank 0  1   16383  0.01
Tcam 0, Bank 1  2   16382  0.01
Tcam 1, Bank 0  7   16377  0.04
Tcam 1, Bank 1  138 16246  0.84
```

For M-series modules, the ACL TCAM is spread across four banks. On non-XL modules, each bank has 16,000 entries for a total of 64K entries. On XL modules each bank has 32,000 entries for a total of 128,000 entries. Under normal circumstances, a single ACL will only use the resources of a single TCAM bank. In order to enable a single ACL to use resources from all of the banks you need to enable bank pooling with the **hardware access-list resource pooling module** *mod-numbe*r command.

You can verify that bank pooling is enabled with the **show hardware access-list resource pooling** command.

ACL TCAM Bank Mapping

ACL ternary control address memory (TCAM) bank mapping allows TCAM banks to accommodate more feature combinations in a more predictable manner. Features are preclassified into feature groups, which are further predefined into feature classes according to which features are allowed to coexist in a TCAM bank. For example, a port ACL (port ACL) feature and a Layer 2 NetFlow feature are defined as one feature class. These classes are allocated to specific banks. An error message appears if you enable or disable a feature class that is not supported on a specific TCAM bank.

ACL TCAM bank mapping allows you to configure a set of features at the same time and reduces multiple results that can accumulate when feature combinations that cannot coexist are configured on the same TCAM banks. By using this feature, you can optimize space and maximize the utilization of TCAM banks.

Beginning with Cisco NX-OS Release 6.2(10), you can issue the **show hardware access-list** {**input** | **output**} {**interface** | **vlan**} **feature-combo** *features* command to display the bank mapping matrix.

Session Manager Support for IP ACLs

Session Manager supports the configuration of IP and MAC ACLs. 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.

Virtualization Support for IP ACLs

The following information applies to IP and MAC ACLs used in virtual device contexts (VDCs):

- ACLs are unique per VDC. You cannot use an ACL that you created in one VDC in a different VDC.
- Because ACLs are not shared by VDCs, you can reuse ACL names in different VDCs.
- The device does not limit ACLs or rules on a per-VDC basis.
- Configuring atomic ACL updates must be performed in the default VDC but applies to all VDCs.

Prerequisites for IP 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.

Guidelines and Limitations for IP ACLs

IP ACLs have the following configuration guidelines and limitations:

- When an access control list (ACL) is applied at the ingress of the original packet, it gets the destination index of the actual egress port and has no knowledge of the Encapsulated Remote Switched Port Analyzer (ERSPAN) session's point of egress at that moment. Because the packet does not go through the ACL engine after rewrite, it cannot be matched on ERSPAN packets.
- 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. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.
- In most cases, ACL processing for IP packets occurs on the I/O modules, which use hardware that accelerates ACL processing. In some circumstances, processing occurs on the supervisor module, which can result in slower ACL processing, especially during processing that involves an ACL with a large number of rules. Management interface traffic is always processed on the supervisor module. If IP packets in any of the following categories are exiting a Layer 3 interface, they are sent to the supervisor module for processing:
    - Packets that fail the Layer 3 maximum transmission unit check and therefore require fragmenting.
    - IPv4 packets that have IP options (additional IP packet header fields following the destination address field).
    - IPv6 packets that have extended IPv6 header fields.

  Rate limiters prevent redirected packets from overwhelming the supervisor module.

  Note Prior to Cisco NX-OS Release 4.2(3), ACL logging does not support ACL processing that occurs on the supervisor module.

- When you apply an ACL that uses time ranges, the device updates the ACL entries on the affected I/O modules whenever a time range referenced in an ACL entry starts or ends. Updates that are initiated by time ranges occur on a best-effort priority. If the device is especially busy when a time range causes an update, the device may delay the update by up to a few seconds.
- To apply an IP ACL to a VLAN interface, you must have enabled VLAN interfaces globally. For more information about VLAN interfaces, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*
- The maximum number of supported IP ACL entries is 64,000 for devices without an XL line card and 128,000 for devices with an XL line card.
- If you try to apply too many ACL entries to a non-XL line card, the configuration is rejected.

The VTY ACL feature restricts all traffic for all VTY lines. You cannot specify different traffic restrictions for different VTY lines.

Any router ACL can be configured as a VTY ACL.

- ACLs configured for VTYs do not apply to the mgmt0 interface. Mgmt0 ACLs must be applied specifically to the interface.
- The Cisco Nexus 2000 Series Fabric Extender supports the full range of ingress ACLs that are available on its parent Cisco Nexus 7000 Series device. For more information about the Fabric Extender, see the *Configuring the Cisco Nexus 2000 Series Fabric Extender*.
- ACL policies are not supported on the Fabric Extender fabric port channel.
- ACL capture is a hardware-assisted feature and is not supported for the management interface or for control packets originating in the supervisor. It is also not supported for software ACLs such as SNMP community ACLs and VTY ACLs.
- Enabling ACL capture disables ACL logging for all VDCs and the rate limiter for ACL logging.
- Port channels and supervisor in-band ports are not supported as a destination for ACL capture.
- ACL capture session destination interfaces do not support ingress forwarding and ingress MAC learning. If a destination interface is configured with these options, the monitor keeps the ACL capture session down. Use the **show monitor session all** command to see if ingress forwarding and MAC learning are enabled.

  Note You can use the **switchport monitor** command to disable ingress forwarding and MAC learning on the interface.

- The source port of the packet and the ACL capture destination port cannot be part of the same packet replication ASIC. If both ports belong to the same ASIC, the packet is not captured. The **show monitor session** command lists all the ports that are attached to the same ASIC as the ACL capture destination port.
- Only one ACL capture session can be active at any given time in the system across VDCs.
- If you configure an ACL capture monitor session before configuring the **hardware access-list capture** command, you must shut down the monitor session and bring it back up in order to start the session.
- When you apply an undefined ACL to an interface, the system treats the ACL as empty and permits all traffic.
- An IPv6 atomic policy update can be disruptive. It may cause disruption when there is an addition, deletion, or modification of an IPv6 source or destination address:
  - Modifying the Layer 4 fields of the IPv6 ACE is not disruptive.
  - Adding an IPv6 address may not always be disruptive, however, it can cause disruption in some cases.
  - There may be disruption if you change the prefix length of an existing entry or add/delete the entry with a new prefix length.

> **Note** An IPv6 atomic policy update is not disruptive for F3 and M3 Series modules.

- Resource pooling and ACL TCAM bank mapping cannot be enabled at the same time.
- You cannot configure the **mac packet-classify** command on shared interfaces.
- M1 Series Modules
    - M1 Series modules support ACL capture.
    - FCoE ACLs are not supported for M1 Series modules.
    - For M1 Series modules, the **mac packet-classify** command enables a MAC ACL for port and VLAN policies.
    - M1 Series modules do not support IP ACLs on port ACL and VACL policies, when the MAC packet classification feature is enabled on the interface. Before you upgrade to Cisco NX-OS Release 6.x or later versions, you need to disable the MAC packet classification feature on M1 Series module and verify whether all the existing functionalities work.
    - M1 Series modules support WCCP.
- M2 Series Modules
    - M2 Series modules support ACL capture.
    - FCoE ACLs are not supported for M2 Series modules.
    - For M2 Series modules, the **mac packet-classify** command enables a MAC ACL for port and VLAN policies.
    - M2 Series modules do not support IP ACLs on port ACL and VACL policies, when the MAC packet classification feature is enabled on the interface. Before you upgrade to Cisco NX-OS Release 6.x or later versions, you need to disable the MAC packet classification feature on M2 Series module and verify whether all the existing functionalities work.
    - M2 Series modules support WCCP.
- F1 Series Modules
    - Each forwarding engine on an F1 Series module supports 1000 ingress ACL entries, with 984 entries available for user configuration. The total number of IP ACL entries for the F1 Series modules is from 1000 to 16,000, depending on which forwarding engines the policies are applied.
    - Each of the 16 forwarding engines in an F1 Series module supports up to 250 IPv6 addresses across multiple ACLs.
    - Each port ACL can support up to four different Layer 4 operations for F1 Series modules.
    - F1 Series modules do not support router ACLs.
    - F1 Series modules do not support ACL logging.
    - F1 Series modules do not support bank chaining.

    - F1 Series modules do not support ACL capture.
    - FCoE ACLs are supported only for F1 Series modules.
    - F1 Series modules do not support WCCP.
    - F1 Series modules do not support ACL TCAM bank mapping.
    - For F1 Series module proxy-forwarded traffic, ACL classification is matched against the Layer 3 protocols shown in the following table:

Table 27: Protocol Number and Associated Layer 3 Protocol

Protocol Number	Layer 3 Protocol
1	ICMP
2	IGMP
4	IPv4 Encapsulation
6	TCP
17	UDP

Note Layer 3 protocols not listed in the table are classified as protocol number 4 (IPv4 Encapsulation).

- F2 Series Modules
    - Each of the 12 forwarding engines in an F2 Series module has 16,000 total TCAM entries, equally split across two banks. 168 default entries are reserved. Each forwarding engine also has 512 IPv6 compression TCAM entries.
    - F2 Series modules do not support ACL capture.
    - For F2 Series modules, the **log** option in egress ACLs is not supported for multicast packets.
    - If an F2 Series module is shared among different VDCs, any egress ACL that is configured on one VDC is pushed to the other VDCs.
    - F2 Series modules do not support egress WCCP on SVI.
    - For F2 Series modules, the **mac packet-classify** command enables a MAC ACL for port policies but an IPv4 or IPv6 ACL for VLAN policies.
- Two banks can be chained within the same TCAM. However, you cannot chain banks across multiple TCAMs.
- The bank chaining and bank mapping features cannot co-exist.
- You cannot configure port ACL features such as PACL, L2 QOS, and L2 Netflow when you enable the VLAN-VLAN mode for configuring the flexible ACL TCAM bank chaining feature.
- The flexible ACL TCAM bank chaining feature is not supported on the F2 Series modules.

- Enabling the flexible ACL TCAM bank chaining feature on all the modules is not supported.
- F3 Series Module
    - The forwarding engines in an F3 Series module has 16,000 total TCAM entries that are equally split across two banks.
    - F3 Series modules supports ACL capture.
    - F3 Series modules supports FCoE ACLs.
    - For F3 Series modules, the log option in egress ACLs is not supported for multicast packets.
    - If an F3 Series module is shared among different VDCs, any egress ACL that is configured on one VDC is pushed to the other VDCs.
    - For F3 Series modules, the **mac packet-classify** command enables a MAC ACL for port policies but an IPv4 or IPv6 ACL for VLAN policies.
    - Two banks can be chained within the same TCAM. However, you cannot chain banks across multiple TCAMs.
    - The bank chaining and bank mapping features cannot co-exist.
    - You cannot configure port ACL features such as PACL, L2 QOS, and L2 Netflow when you enable the VLAN-VLAN mode for configuring the flexible ACL TCAM bank chaining feature.
    - The flexible ACL TCAM bank chaining feature is supported only on the F3 Series modules. Enabling the flexible ACL TCAM bank chaining feature on all the modules is not supported.

ACLs on VTY lines have the following guidelines and limitations:

- ACLs applied on a VTY line in egress direction filter traffic without any issues. However, ACLs applied on a VTY line in ingress direction will not filter management traffic. For example, FTP, TFTP, or SFP traffic in the return direction, that is, if the FTP connection is initiated from a switch to an external server, ingress ACL on a VTY line will not be used, if ACLs are configured to block or permit this return traffic. Therefore, ACLs should be applied in the egress direction on VTY lines to block the FTP, TFTP, or SCP traffic from the switch.
- It is recommended to use ACLs on management interface as well to secure access to the switch from secured and permitted sources.

Default Settings for IP ACLs

This table lists the default settings for IP ACL parameters.

Table 28: Default IP ACL Parameters

Parameters	Default
IP ACLs	No IP ACLs exist by default
ACL rules	Implicit rules apply to all ACLs
ACL capture	Disabled

Parameters	Default
Object groups	No object groups exist by default
Time ranges	No time ranges exist by default
ACL TCAM bank mapping	Disabled

Related Topics

Implicit Rules for IP and MAC ACLs, on page 410

Configuring IP ACLs

Creating an IP ACL

You can create an IPv4 ACL or IPv6 ACL on the device and add rules to it.

Before you begin

We recommend that you perform the ACL configuration using the Session Manager. This feature allows you to verify the ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. This feature is especially useful for ACLs that include more than about 1000 rules. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
   - **ip access-list** *name*
   - **ipv6 access-list** *name*
3. (Optional) **fragments** {**permit-all** | **deny-all**}
4. [*sequence-number*] {**permit** | **deny**} *protocol source destination*
5. (Optional) **statistics per-entry**
6. (Optional) Enter one of the following commands:
   - **show ip access-lists** *name*
   - **show ipv6 access-lists** *name*
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	Enter one of the following commands:
	• **ip access-list** *name*
	• **ipv6 access-list** *name*
	Example:
	`switch(config)# ip access-list acl-01`
	`switch(config-acl)#`
		Creates the IP ACL and enters IP ACL configuration mode. The *name* argument can be up to 64 characters. From Cisco NX-OS Release 8.4(2), the name argument can be upto 256 characters.

Step 3	(Optional) **fragments** {**permit-all** | **deny-all**} **Example:** `switch(config-acl)# fragments permit-all`	Optimizes fragment handling for noninitial fragments. When a device applies to traffic an ACL that contains the **fragments** command, the **fragments** command only matches noninitial fragments that do not match any explicit **permit** or **deny** commands in the ACL.
Step 4	[*sequence-number*] {**permit** | **deny**} *protocol source destination* **Example:** `switch(config-acl)# permit ip 192.168.2.0/24 any`	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 *Cisco Nexus 7000 Series NX-OS Security Command Reference*.
Step 5	(Optional) **statistics per-entry** **Example:** `switch(config-acl)# statistics per-entry`	Specifies that the device maintains global statistics for packets that match the rules in the ACL.
Step 6	(Optional) Enter one of the following commands: • **show ip access-lists** *name* • **show ipv6 access-lists** *name* **Example:** `switch(config-acl)# show ip access-lists acl-01`	Displays the IP ACL configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config-acl)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Changing an IP ACL

You can add and remove rules in an existing IPv4 or IPv6 ACL, but 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.

Before you begin

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 feature is especially useful for ACLs that include more than about 1000 rules. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
   - **ip access-list** *name*
   - **ipv6 access-list** *name*
3. (Optional) [*sequence-number*] {**permit** | **deny**} *protocol source destination*
4. (Optional) [**no**] **fragments** {**permit-all** | **deny-all**}
5. (Optional) **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*}
6. (Optional) [**no**] **statistics per-entry**
7. (Optional) Enter one of the following commands:
   - **show ip access-lists** *name*
   - **show ipv6 access-lists** *name*
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	Enter one of the following commands:
	• **ip access-list** *name*
	• **ipv6 access-list** *name*
	Example:
	`switch(config)# ip access-list acl-01`
	`switch(config-acl)#`
		Enters IP ACL configuration mode for the ACL that you specify by name.

Step 3	(Optional) [*sequence-number*] {**permit** | **deny**} *protocol source destination* **Example:** `switch(config-acl)# 100 permit ip 192.168.2.0/24 any`	Creates a rule in the IP ACL. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the 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 *Cisco*

	Command or Action	Purpose
		Nexus 7000 Series NX-OS System Management Configuration Guide.
Step 4	(Optional) [**no**] **fragments** {**permit-all** | **deny-all**} **Example:** `switch(config-acl)# fragments permit-all`	Optimizes fragment handling for noninitial fragments. When a device applies to traffic an ACL that contains the **fragments** command, the **fragments** command only matches noninitial fragments that do not match any explicit **permit** or **deny** commands in the ACL. The **no** option removes fragment-handling optimization.
Step 5	(Optional) **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*} **Example:** `switch(config-acl)# no 80`	Removes the rule that you specified from the IP ACL. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.
Step 6	(Optional) [**no**] **statistics per-entry** **Example:** `switch(config-acl)# statistics per-entry`	Specifies that the device maintains global statistics for packets that match the rules in the ACL. The **no** option stops the device from maintaining global statistics for the ACL.
Step 7	(Optional) Enter one of the following commands: • **show ip access-lists** *name* • **show ipv6 access-lists** *name* **Example:** `switch(config-acl)# show ip access-lists acl-01`	Displays the IP ACL configuration.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config-acl)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Changing Sequence Numbers in an IP ACL, on page 431

Creating a VTY ACL

You can configure a VTY ACL to control access to all IPv4 or IPv6 traffic over all VTY lines in the ingress or egress direction.

Before you begin

Set identical restrictions on all the virtual terminal lines because a user can connect to any of them.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

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, which is especially useful for ACLs that include more than about 1000 rules. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.

SUMMARY STEPS

1. **configure terminal**
2. {**ip** | **ipv6**} **access-list** *name*
3. {**permit** | **deny**} *protocol source destination* [**log**] [**time-range** *time*]
4. **exit**
5. **line vty**
6. {**ip** | **ipv6**} **access-class** *name* {**in** | **out**}
7. (Optional) **show** {**ip** | **ipv6**} **access-lists**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	{**ip** | **ipv6**} **access-list** *name* **Example:** `switch(config)# ip access-list vtyacl`	Creates an ACL and enters IP access list configuration mode for that ACL. The maximum length for the *name* argument is 64 characters.
Step 3	{**permit** | **deny**} *protocol source destination* [**log**] [**time-range** *time*] **Example:** `switch(config-ip-acl)# permit tcp any any`	Creates an ACL rule that permits TCP traffic from and to the specified sources.

Step 4	**exit**
	Example:
	`switch(config-ip-acl)# exit`
	`switch(config)#`
		Exits IP access list configuration mode.

Step 5	**line vty**
	Example:
	`switch(config)# line vty`
	`switch(config-line)#`
		Specifies the virtual terminal and enters line configuration mode.

Step 6	{**ip** | **ipv6**} **access-class** *name* {**in** | **out**} **Example:** `switch(config-line)# ip access-class vtyacl out`	Restricts incoming or outgoing connections to and from all VTY lines using the specified ACL. The maximum length for the *name* argument is 64 characters.

	Command or Action	Purpose
Step 7	(Optional) **show** {**ip** | **ipv6**} **access-lists** **Example:** `switch# show ip access-lists`	Displays the configured ACLs, including any VTY ACLs.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Changing Sequence Numbers in an IP ACL

You can change all the sequence numbers assigned to the rules in an IP ACL.

Before you begin

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 feature is especially useful for ACLs that include more than about 1000 rules. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.

SUMMARY STEPS

1. **configure terminal**
2. **resequence** {**ip** | **ipv6**} **access-list** *name starting-sequence-number increment*
3. (Optional) **show ip access-lists** *name*
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**resequence** {**ip** | **ipv6**} **access-list** *name starting-sequence-number increment* **Example:** `switch(config)# resequence access-list ip acl-01 100 10`	Assigns sequence numbers to the rules contained in the ACL, where the first rule receives the starting sequence number that you specify. Each subsequent rule receives a number larger than the preceding rule. The difference in numbers is determined by the increment that you specify. The *starting-sequence-number* argument and the *increment* argument can be a whole number between 1 and 4294967295.
Step 3	(Optional) **show ip access-lists** *name* **Example:**	Displays the IP ACL configuration.

	Command or Action	Purpose
	`switch(config)# show ip access-lists acl-01`	
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Removing an IP ACL

You can remove an IP ACL from the device.

Before you begin

Ensure that you know whether the ACL is applied to an interface. The device 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 device considers the removed ACL to be empty. Use the **show ip access-lists** command or the **show ipv6 access-lists** command with the summary keyword to find the interfaces that an IP ACL is configured on.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
    - **no ip access-list** *name*
    - **no ipv6 access-list** *name*
3. (Optional) Enter one of the following commands:
    - **show ip access-lists** *name* **summary**
    - **show ipv6 access-lists** *name* **summary**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	Enter one of the following commands: • **no ip access-list** *name* • **no ipv6 access-list** *name* **Example:** `switch(config)# no ip access-list acl-01`	Removes the IP ACL that you specified by name from the running configuration.

	Command or Action	Purpose
Step 3	(Optional) Enter one of the following commands: • **show ip access-lists** *name* **summary** • **show ipv6 access-lists** *name* **summary** **Example:** `switch(config)# show ip access-lists acl-01 summary`	Displays the IP ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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

ACLs applied to these interface types are considered router ACLs.

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.

SUMMARY STEPS

1. switch# **configure terminal**
2. Enter one of the following commands:
   - switch(config)# **interface ethernet** *slot*/*port*[**.** *number*]
   - switch(config)# **interface port-channel** *channel-number*[**.** *number*]
   - switch(config)# **interface tunnel** *tunnel-number*
   - switch(config)# **interface vlan** *vlan-ID*
   - switch(config)# **interface mgmt** *port*
3. Enter one of the following commands:
   - switch(config-if)# **ip access-group** *access-list* {**in** | **out**}
   - switch(config-if)# **ipv6 traffic-filter** *access-list* {**in** | **out**}
4. (Optional) switch(config-if)# **show running-config aclmgr**

5. (Optional) switch(config-if)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	Enter one of the following commands: • switch(config)# **interface ethernet** *slot*/*port*[**.** *number*] • switch(config)# **interface port-channel** *channel-number*[**.** *number*] • switch(config)# **interface tunnel** *tunnel-number* • switch(config)# **interface vlan** *vlan-ID* • switch(config)# **interface mgmt** *port*	Enters configuration mode for the interface type that you specified.
Step 3	Enter one of the following commands: • switch(config-if)# **ip access-group** *access-list* {**in** | **out**} • switch(config-if)# **ipv6 traffic-filter** *access-list* {**in** | **out**}	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.
Step 4	(Optional) switch(config-if)# **show running-config aclmgr**	Displays the ACL configuration.
Step 5	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Related Topics

Creating an IP ACL, on page 426

Applying an IP ACL as a Port ACL

You can apply an IPv4 or IPv6 ACL to a Layer 2 interface, which can be a physical port or a port channel. ACLs applied to these interface types are considered port ACLs.

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.

Note If the interface is configured with the **mac packet-classify** command, you cannot apply an IP port ACL to the interface until you remove the **mac packet-classify** command from the interface configuration.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:

- **interface ethernet** *slot*/*port*
- **interface port-channel** *channel-number*

3. Enter one of the following commands:
    - **ip port access-group** *access-list* **in**
    - **ipv6 port traffic-filter** *access-list* **in**
4. (Optional) **show running-config aclmgr**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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 2/3`
	`switch(config-if)#`
		Enters configuration mode for the interface type that you specified.

Step 3	Enter one of the following commands:
	• **ip port access-group** *access-list* **in**
	• **ipv6 port traffic-filter** *access-list* **in**
	Example:
	`switch(config-if)# ip port access-group`
	`acl-l2-marketing-group in`
		Applies an IPv4 or IPv6 ACL to the interface or port channel. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.

Step 4	(Optional) **show running-config aclmgr** **Example:** `switch(config-if)# show running-config aclmgr`	Displays the ACL configuration.

Step 5	(Optional) **copy running-config startup-config**
	Example:
	`switch(config-if)# copy running-config`
	`startup-config`
		Copies the running configuration to the startup configuration.

Related Topics

Creating an IP ACL, on page 426
Enabling or Disabling MAC Packet Classification, on page 468

Applying an IP ACL as a VACL

You can apply an IP ACL as a VACL.

Related Topics

Configuring VACLs, on page 476

Enabling or Disabling ACL Capture

Beginning with Cisco NX-OS Release 5.2, you can enable or disable ACL capture in the default VDC.

Before you begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **hardware access-list capture**
3. (Optional) **show hardware access-list status module** *slot*
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **hardware access-list capture** **Example:** `switch(config)# hardware access-list capture`	Enables or disables ACL capture on all VDCs. **Note** When you enable ACL capture, a warning message appears to inform you that ACL logging is being disabled for all VDCs. When you disable ACL capture, ACL logging is enabled.
Step 3	(Optional) **show hardware access-list status module** *slot* **Example:** `switch(config)# show hardware access-list status module 2`	Displays the ACL capture 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.

Related Topics

ACL Capture, on page 415

Configuring an ACL Capture Session

Beginning with Cisco NX-OS Release 5.2, you can configure an ACL capture session.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**
2. **monitor session** *session* **type acl-capture**
3. **destination interface** *interface slot/port*
4. **no shut**
5. **exit**
6. (Optional) **show ip access-lists capture session** *session*
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**monitor session** *session* **type acl-capture**
	Example:
	`switch(config)# monitor session 2 type acl-capture`
	`switch(config-acl-capture)#`
		Configures an ACL capture session. The range for the *session* argument is from 1 to 48.

Step 3	**destination interface** *interface slot/port*
	Example:
	`switch(config-acl-capture)# destination interface ethernet 2/2`
	`switch#`
		Configures a destination for ACL capture packets.
		Note Only the physical interface can be used for the destination. Port-channel interfaces and supervisor in-band ports are not supported.
		Note You can enter this command multiple times to add multiple destinations.

Step 4	**no shut** **Example:** `switch(config-acl-capture)# no shut`	Brings the ACL capture session administratively up. **Note** The session becomes operationally up only after the monitor confirms that the ACL capture has been enabled in the default VDC.

	Command or Action	Purpose

Step 5	**exit**
	Example:
	`switch(config-acl-capture)# exit`
	`switch(config)#`
		Updates the monitor configuration and exits the ACL capture configuration mode.

Step 6	(Optional) **show ip access-lists capture session** *session* **Example:** `switch(config)# show ip access-lists capture session 2`	Displays the ACL capture session configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Applying an ACL with Capture Session ACEs to an Interface

You can enable a capture session for an ACL's access control entries (ACEs) and then apply the ACL to an interface.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**
2. **ip access-list** *name*
3. **permit** *protocol source destination* **capture session** *session*
4. **exit**
5. **interface** *interface slot/port*
6. **ip access-group** *name* **in**
7. **no shut**
8. (Optional) **show running-config aclmgr**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip access-list** *name* **Example:**	Creates an access list.

	Command or Action	Purpose
	`switch(config)# ip access-list acl1` `switch(config-acl)#`	
Step 3	**permit** *protocol source destination* **capture session** *session* **Example:** `switch(config-acl)# permit tcp any any capture session 2`	Enables a capture session for the ACL's ACEs. The range for the *session* argument is from 1 to 16.

Step 4	**exit**
	Example:
	`switch(config-acl)# exit`
	`switch(config)#`
		Exits the access list configuration mode.

Step 5	**interface** *interface slot*/*port*
	Example:
	`switch(config)# interface ethernet 7/1`
	`switch(config-if)#`
		Specifies a port and enters interface configuration mode.

Step 6	**ip access-group** *name* **in** **Example:** `switch(config-if)# ip access-group acl1 in`	Applies an ACL with capture session ACEs to the interface.
Step 7	**no shut** **Example:** `switch(config-if)# no shut`	Brings the interface administratively up.
Step 8	(Optional) **show running-config aclmgr** **Example:** `switch(config-if)# show running-config aclmgr`	Displays the ACL configuration and the interfaces to which ACLs are applied.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Applying a Whole ACL Capture Session to an Interface

You can enable a capture session for the whole ACL and then apply the ACL to an interface.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**
2. **ip access-list** *name*

3. **capture session** *session*
4. **exit**
5. **interface** *interface slot*/*port*
6. **ip access-group** *name* **in**
7. **no shut**
8. (Optional) **show running-config aclmgr**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip access-list** *name*
	Example:
	`switch(config)# ip access-list acl1`
	`switch(config-acl)#`
		Creates an access list.

Step 3	**capture session** *session* **Example:** `switch(config-acl)# capture session 2`	Enables a capture session for the whole ACL. The range for the *session* argument is from 1 to 16.

Step 4	**exit**
	Example:
	`switch(config-acl)# exit`
	`switch(config)#`
		Exits the access list configuration mode.

Step 5	**interface** *interface slot*/*port*
	Example:
	`switch(config)# interface ethernet 7/1`
	`switch(config-if)#`
		Specifies a port and enters interface configuration mode.

Step 6	**ip access-group** *name* **in** **Example:** `switch(config-if)# ip access-group acl1 in`	Applies an ACL with the capture session configuration to the interface.
Step 7	**no shut** **Example:** `switch(config-if)# no shut`	Brings the interface administratively up.
Step 8	(Optional) **show running-config aclmgr** **Example:** `switch(config-if)# show running-config aclmgr`	Displays the ACL configuration and the interfaces to which ACLs are applied.

	Command or Action	Purpose
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Scale ACL

Scale ACL is introduced in Cisco NX-OS Release 8.4(2) and it is supported on M3 modules. This feature support is added only for RACL policies with object-group. This feature helps you to implement large scale configuration of ACL with support of object-group configuration. Both IPv4 and IPv6 RACL is supported. Scale ACL is configured with the key word, **compress**.

SUMMARY STEPS

1. **configure terminal**
2. **[no] hardware access-list compress module** *module-number*
3. **interface** *interface-name number*
4. **[no] ip access-group access-list** {**in** | **out** } **compress**
5. **end**
6. **show ip access-list** *name* **compress**
7. **show hardware access-list compress**
8. **show system internal access-list resource presearch-utilization**
9. **show system internal access-list interface** *interface-name number* **input presearch-entries**
10. **show system internal access-list interface** *interface-name number* **input statistics**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**[no] hardware access-list compress module** *module-number* **Example:** `switch(config)# hardware access-list compress module 2`	Configures Scale ACL on a module. Reload the module after configuring the scale ACL.
Step 3	**interface** *interface-name number* **Example:** `switch(config)# interface port-channel 1`	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	**[no] ip access-group access-list** {**in** | **out** } **compress** **Example:** `switch(config-if)# ip access-group test in compress`	Configures access list on an interface and applies the scale ACL. You can apply access-list only when the “statistics per-entry” is enabled.
Step 5	**end** **Example:** `switch(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.
Step 6	**show ip access-list** *name* **compress** **Example:** `switch# show ip access-list test compress`	Displays the scale ACL statistics.
Step 7	**show hardware access-list compress** **Example:** `switch# show hardware access-list compress`	Displays the M3 modules on which the compression is enabled.
Step 8	**show system internal access-list resource presearch-utilization** **Example:** `switch# show system internal access-list resource presearch-utilization`	Displays the pre-search TCAM utilization information.
Step 9	**show system internal access-list interface** *interface-name number* **input presearch-entries** **Example:** `switch# show system internal access-list interface port-channel 1 input presearch-entries`	Displays information on the IP programmed in pre-search TCAM for a policy.
Step 10	**show system internal access-list interface** *interface-name number* **input statistics** **Example:** `switch# show system internal access-list interface port-channel 1 input statistics`	Displays information on the TCAM programming for a policy.

Configuration Examples for Scale ACL

The following example shows the M3 module on which the compression is enabled:

```
switch# show hardware access-list compress
+------------+--------------+---------------+
| MODULE_NUM | CONFIG_STATUS | RUNTIME_STATUS |
+------------+--------------+---------------+
| 1 |              No |        Inactive |
+------------+--------------+---------------+
```

The following example displays the ACL statistics:

```
switch# show ip access-lists test compress
IP access list test
statistics per-entry
10 permit ip addrgroup G1 addrgroup G2 fragments log [match=1833318182]
20 permit ip addrgroup G1 addrgroup G3 dscp af21 log [match=1833318182]
30 permit ip addrgroup G1 addrgroup G3 precedence critical log [match=1833318182]
40 permit ip addrgroup G1 addrgroup G2 dscp af11 log [match=1833318181]
50 permit ip addrgroup G1 addrgroup G2 dscp af12 log [match=0]
60 permit ip addrgroup G1 addrgroup G2 dscp af13 log [match=0]
70 permit ip addrgroup G1 addrgroup G2 dscp af22 log [match=0]
80 permit ip addrgroup G1 addrgroup G2 dscp af23 packet-length neq 9010 log [match=0]
```

The following example displays the pre-search TCAM utilization information.

```
switch# show system internal access-list resource presearch-utilization
INSTANCE 0x0
-------------
Presearch-SA ACL Hardware Resource Utilization (Mod 1)
--------------------------------------------
Used Free Percent
Utilization
-----------------------------------------------------
Tcam 0, Bank 0 0 16384 0.00
Tcam 0, Bank 1 0 16384 0.00
Tcam 1, Bank 0 0 16384 0.00
Tcam 1, Bank 1 80 16304 0.49
Presearch-DA ACL Hardware Resource Utilization (Mod 1)
--------------------------------------------
Used Free Percent
Utilization
-----------------------------------------------------
Tcam 0, Bank 0 0 16384 0.00
Tcam 0, Bank 1 0 16384 0.00
Tcam 1, Bank 0 0 16384 0.00
Tcam 1, Bank 1 67 16317 0.41
```

The following example shows how to verify the IP programmed in pre-search TCAM for a policy:

```
switch# show system internal access-list interface port-channel 1 input presearch-entries

INSTANCE 0x0
---------------
Tcam 0 resource usage:
----------------------
Presearch-SA
------------
Label_a = 0x2
Bank 0
------
IPv4 Class
Policies: RACL(test_acl)
Entries:
[Index] Entry [Result]
---------------------
[0000:257042:0000] 1.1.1.1/32 [0x2000000]
[0001:256882:0001] 1.1.1.2/32 [0x2000000]
[0002:2568c2:0002] 1.1.1.3/32 [0x2000000]
[0003:256942:0003] 5.5.5.37/32 [0x2000000]
[0004:256a02:0004] 6.6.6.40/32 [0x2000000]
[0005:256e82:0005] 10.10.10.10/32 [0x2000000]
[0006:256902:0006] 20.20.20.20/32 [0x1000000]
[0007:2569c2:0007] 23.23.23.23/32 [0x1000000]
[0008:256c42:0008] 192.168.1.1/32 [0x3000000]
[0009:256c82:0009] 192.168.1.2/32 [0x3000000]
[000a:256cc2:000a] 192.168.1.3/32 [0x3000000]
```

```
[000b:257502:000b] 192.168.1.4/32 [0x3000000]
Bank 1
------
IPv4 Class
Policies: RACL(test_acl)
Entries:
[Index] Entry [Result]
---------------------
[0000:256842:0000] 1.1.1.1/32 [0x2000000]
[0001:257082:0001] 1.1.1.2/32 [0x2000000]
[0002:2570c2:0002] 1.1.1.3/32 [0x2000000]
[0003:257142:0003] 5.5.5.37/32 [0x2000000]
[0004:257202:0004] 6.6.6.40/32 [0x2000000]
[0005:257682:0005] 10.10.10.10/32 [0x2000000]
[0006:257102:0006] 20.20.20.20/32 [0x1000000]
[0007:2571c2:0007] 23.23.23.23/32 [0x1000000]
[0008:257442:0008] 192.168.1.1/32 [0x3000000]
[0009:257482:0009] 192.168.1.2/32 [0x3000000]
[000a:2574c2:000a] 192.168.1.3/32 [0x3000000]
[000b:256d02:000b] 192.168.1.4/32 [0x3000000]
```

The following example shows how to verify the main TCAM programming for a policy:

```
switch# show system internal access-list interface port-channel 1 input statistics
INSTANCE 0x0
---------------
Tcam 0 resource usage:
----------------------
Label_a = 0x1
Bank 0
------
IPv4 Class
Policies: RACL(test_acl)
Netflow profile: 0
Netflow deny profile: 0
Entries:
[Index] Entry [Stats]
---------------------
[0014:436a2:0000] prec 2 objgrp-permit-routed ip 0x1000000/0x7000000 0x3000000/0x3000000
[3545]
[0015:43722:0001] prec 2 objgrp-permit-routed ip 0x2000000/0x7000000 0x1000000/0x3000000
[0]
[0016:437a2:0002] prec 2 objgrp-permit-routed ip 0x3000000/0x7000000 0x2000000/0x3000000
[0]
[0017:3c222:0003] prec 2 objgrp-permit-routed ip 0x4000000/0x7000000 0x4000000/0x4000000
[0]
[0018:43222:0004] prec 2 deny-routed ip 0x0/0x0 0x0/0x0 [0]
```

Verifying the IP ACL Configuration

To display IP ACL configuration information, perform one of the following tasks. For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
show hardware access-list status module *slot*	Displays the ACL capture configuration.

Command	Purpose
show ip access-lists [**capture session** *session*]	Displays the IPv4 ACL configuration.
show ipv6 access-lists [**capture session** *session*]	Displays the IPv6 ACL configuration.
show system internal access-list feature bank-class map {**ingress** | **egress**} [**module** *module*]	Displays the feature group and class combination tables.
show running-config aclmgr [**all**]	Displays the ACL running configuration, including the IP ACL configuration and the interfaces to which IP ACLs are applied. **Note** Beginning with Cisco NX-OS Release 5.2, this command displays the user-configured ACLs in the running configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
show startup-config aclmgr [**all**]	Displays the ACL startup configuration. **Note** Beginning with Cisco NX-OS Release 5.2, this command displays the user-configured ACLs in the startup configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

Note If TCP permits or deny in the ACL, the **ip access-list detailed** command doesn't identify established conditions. The traffic is counted for ACL if other condition matches though a successful TCP connection is not established. Detailed log entries will not be displayed (this is only for the ACL logging and does not include or affect the actual ACL forwarding decision).

Monitoring and Clearing IP ACL Statistics

To monitor or clear IP ACL statistics, use one of the commands in this table. For detailed information about these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
show ip access-lists	Displays the IPv4 ACL configuration. If the IPv4 ACL includes the **statistics per-entry** command, the **show ip access-lists** command output includes the number of packets that have matched each rule.
show ipv6 access-lists	Displays IPv6 ACL configuration. If the IPv6 ACL includes the **statistics per-entry** command, then the **show ipv6 access-lists** command output includes the number of packets that have matched each rule.
clear ip access-list counters	Clears statistics for all IPv4 ACLs or for a specific IPv4 ACL.
clear ipv6 access-list counters	Clears statistics for all IPv6 ACLs or for a specific IPv6 ACL.

Configuration Examples for IP ACLs

The following example shows how to create an IPv4 ACL named acl-01 and apply it as a port ACL to Ethernet interface 2/1, which is a Layer 2 interface:

```
ip access-list acl-01
  permit ip 192.168.2.0/24 any
interface ethernet 2/1
  ip port access-group acl-01 in
```

The following example shows how to create an IPv6 ACL named acl-120 and apply it as a router ACL to Ethernet interface 2/3, which is a Layer 3 interface:

```
ipv6 access-list acl-120
  permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
interface ethernet 2/3
  ipv6 traffic-filter acl-120 in
```

The following example shows how to create a VTY ACL named single-source and apply it on input IP traffic over the VTY line. This ACL allows all TCP traffic through and drops all other IP traffic:

```
ip access-list single-source
  permit tcp 192.168.7.5/24 any
  exit
  line vty
  ip access-class single-source in
  show ip access-lists
```

The following example shows how to enable ACL capture in the default VDC and configure a destination for ACL capture packets:

```
hardware access-list capture
  monitor session 1 type acl-capture
  destination interface ethernet 2/1
  no shut
  exit
  show ip access-lists capture session 1
```

The following example shows how to enable a capture session for an ACL's access control entries (ACEs) and then apply the ACL to an interface:

```
ip access-list acl1
  permit tcp any any capture session 1
  exit
  interface ethernet 1/11
  ip access-group acl1 in
  no shut
  show running-config aclmgr
```

The following example shows how to apply an ACL with capture session access control entries (ACEs) to a VLAN:

```
vlan access-map acl-vlan-first
  match ip address acl-ipv4-first
  match mac address acl-mac-first
  action foward
  statistics per-entry
  vlan filter acl-vlan-first vlan-list 1
  show running-config vlan 1
```

The following example shows how to enable a capture session for the whole ACL and then apply the ACL to an interface:

```
ip access-list acl2
  capture session 2
  exit
  interface ethernet 7/1
  ip access-group acl1 in
  no shut
  show running-config aclmgr
```

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.

SUMMARY STEPS

1. **configure terminal**
2. **object-group ip address** *name*
3. Enter one of the following commands:
    - [*sequence-number*] **host** *IPv4-address*
    - [*sequence-number*] *IPv4-address network-wildcard*
    - [*sequence-number*] *IPv4-address/prefix-len*
4. Enter one of the following commands:
    - **no** [*sequence-number*]
    - **no host** *IPv4-address*
    - **no** *IPv4-address network-wildcard*
    - **no** *IPv4-address/prefix-len*
5. (Optional) **show object-group** *name*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**object-group ip address** *name*
	Example:
	`switch(config)# object-group ip address ipv4-addr-group-13`
	`switch(config-ipaddr-ogroup)#`
		Creates the IPv4 address object group and enters IPv4 address object-group configuration mode.

Step 3	Enter one of the following commands: • [*sequence-number*] **host** *IPv4-address* • [*sequence-number*] *IPv4-address network-wildcard* • [*sequence-number*] *IPv4-address/prefix-len* **Example:** `switch(config-ipaddr-ogroup)# host 10.99.32.6`	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 to specify a network of hosts.
Step 4	Enter one of the following commands: • **no** [*sequence-number*] • **no host** *IPv4-address* • **no** *IPv4-address network-wildcard* • **no** *IPv4-address/prefix-len* **Example:** `switch(config-ipaddr-ogroup)# no host 10.99.32.6`	Removes an entry in the object group. For each entry that you want to remove from the object group, use the **no** form of the **host** command.

	Command or Action	Purpose
Step 5	(Optional) **show object-group** *name* **Example:** `switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13`	Displays the object group configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-ipaddr-ogroup)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Creating and Changing an IPv6 Address Object Group

You can create and change an IPv6 address group object.

SUMMARY STEPS

1. **config t**
2. **object-group ipv6 address** *name*
3. Enter one of the following commands:
   - [*sequence-number*] **host** *IPv6-address*
   - [*sequence-number*] *IPv6-address*/*prefix-len*
4. Enter one of the following commands:
   - **no** *sequence-number*
   - **no host** *IPv6-address*
   - **no** *IPv6-address*/*prefix-len*
5. (Optional) **show object-group** *name*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**object-group ipv6 address** *name*
	Example:
	`switch(config)# object-group ipv6 address ipv6-addr-group-A7`
	`switch(config-ipv6addr-ogroup)#`
		Creates the IPv6 address object group and enters IPv6 address object-group configuration mode.

	Command or Action	Purpose
Step 3	Enter one of the following commands: • [*sequence-number*] **host** *IPv6-address* • [*sequence-number*] *IPv6-address/prefix-len* **Example:** `switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1`	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.
Step 4	Enter one of the following commands: • **no** *sequence-number* • **no host** *IPv6-address* • **no** *IPv6-address/prefix-len* **Example:** `switch(config-ipv6addr-ogroup)# no host 2001:db8:0:3ab0::1`	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.
Step 5	(Optional) **show object-group** *name* **Example:** `switch(config-ipv6addr-ogroup)# show object-group ipv6-addr-group-A7`	Displays the object group configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-ipv6addr-ogroup)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Creating and Changing a Protocol Port Object Group

You can create and change a protocol port object group.

SUMMARY STEPS

1. **configure terminal**
2. **object-group ip port** *name*
3. [*sequence-number*] *operator port-number* [*port-number*]
4. **no** {*sequence-number* | *operator port-number* [*port-number*]}
5. (Optional) **show object-group** *name*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**object-group ip port** *name*
	Example:
	`switch(config)# object-group ip port NYC-datacenter-ports`
	`switch(config-port-ogroup)#`
		Creates the protocol port object group and enters port object-group configuration mode.

Step 3	[*sequence-number*] *operator port-number* [*port-number*] **Example:** `switch(config-port-ogroup)# eq 80`	Creates an entry in the object group. For each entry that you want to create, use one of the following operator commands: • **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. • **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.
Step 4	**no** {*sequence-number* | *operator port-number* [*port-number*]} **Example:** `switch(config-port-ogroup)# 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-ogroup)# show object-group NYC-datacenter-ports`	Displays the object group configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-port-ogroup)# 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.

SUMMARY STEPS

1. **configure terminal**
2. **no object-group** {**ip address** | **ipv6 address** | **ip port**} *name*
3. (Optional) **show object-group**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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.
Step 3	(Optional) **show object-group** **Example:** `switch(config)# show object-group`	Displays all object groups. The removed object group should not appear.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the Object-Group Configuration

To display object-group configuration information, perform one of the following tasks:

Command	Purpose
show object-group	Displays the object-group configuration.
show running-config aclmgr	Displays ACL configuration, including object groups.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuring Time Ranges

Session Manager Support for Time Ranges

Session Manager supports the configuration of time ranges. This feature allows you to create a configuration session and verify your time-range 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 a Time Range

You can create a time range on the device and add rules to it.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command). Because ACL names can be repeated in different VDCs, we recommend that you confirm which VDC you are working in.

SUMMARY STEPS

1. **configure terminal**
2. **time-range** *name*
3. (Optional) [*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time*
4. (Optional) [*sequence-number*] **periodic** *list-of-weekdays time* **to** *time*
5. (Optional) [*sequence-number*] **absolute start** *time date* [**end** *time date*]
6. (Optional) [*sequence-number*] **absolute** [start *time date*] **end** *time date*
7. (Optional) **show time-range** *name*
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**time-range** *name*
	Example:
	`switch(config)# time-range workday-daytime`
	`switch(config-time-range)#`
		Creates the time range and enters time-range configuration mode.

Step 3	(Optional) [*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time* **Example:**	Creates a periodic rule that is in effect for one or more contiguous days between and including the specified start and end days and times.

	Command or Action	Purpose
	`switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59`	
Step 4	(Optional) [*sequence-number*] **periodic** *list-of-weekdays time* **to** *time* **Example:** `switch(config-time-range)# periodic weekdays 06:00:00 to 20:00:00`	Creates a periodic rule that is in effect on the days specified by the *list-of-weekdays* argument between and including the specified start and end times. The following keywords are also valid values for the *list-of-weekdays* argument: • **daily** —All days of the week. • **weekdays** —Monday through Friday. • **weekend** —Saturday through Sunday.
Step 5	(Optional) [*sequence-number*] **absolute start** *time date* [**end** *time date*] **Example:** `switch(config-time-range)# absolute start 1:00 15 march 2008`	Creates an absolute rule that is in effect beginning at the time and date specified after the **start** keyword. If you omit the **end** keyword, the rule is always in effect after the start time and date have passed.
Step 6	(Optional) [*sequence-number*] **absolute** [start *time date*] **end** *time date* **Example:** `switch(config-time-range)# absolute end 23:59:59 31 december 2008`	Creates an absolute rule that is in effect until the time and date specified after the **end** keyword. If you omit the **start** keyword, the rule is always in effect until the end time and date have passed.
Step 7	(Optional) **show time-range** *name* **Example:** `switch(config-time-range)# show time-range workday-daytime`	Displays the time-range configuration.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config-time-range)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Changing a Time Range

You can add and remove rules in an existing time range. 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.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command). Because ACL names can be repeated in different VDCs, we recommend that you confirm which VDC you are working in.

SUMMARY STEPS

1. **configure terminal**
2. **time-range** *name*
3. (Optional) [*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time*
4. (Optional) [*sequence-number*] **periodic** *list-of-weekdays time* **to** *time*
5. (Optional) [*sequence-number*] **absolute start** *time date* [**end** *time date*]
6. (Optional) [*sequence-number*] **absolute** [**start** *time date*] **end** *time date*
7. (Optional) **no** {*sequence-number* | **periodic** *arguments* . . . | **absolute** *arguments*. . .}
8. (Optional) **show time-range** *name*
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**time-range** *name*
	
	Example:
	`switch(config)# time-range workday-daytime`
	`switch(config-time-range)#`
		Enters time-range configuration mode for the specified time range.

Step 3	(Optional) [*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time* **Example:** `switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59`	Creates a periodic rule that is in effect for one or more contiguous days between and including the specified start and end days and times.
Step 4	(Optional) [*sequence-number*] **periodic** *list-of-weekdays time* **to** *time* **Example:** `switch(config-time-range)# 100 periodic weekdays 05:00:00 to 22:00:00`	Creates a periodic rule that is in effect on the days specified by the *list-of-weekdays* argument between and including the specified start and end times. The following keywords are also valid values for the *list-of-weekdays* argument: • **daily** —All days of the week. • **weekdays** —Monday through Friday. • **weekend** —Saturday through Sunday.
Step 5	(Optional) [*sequence-number*] **absolute start** *time date* [**end** *time date*] **Example:** `switch(config-time-range)# absolute start 1:00 15 march 2008`	Creates an absolute rule that is in effect beginning at the time and date specified after the **start** keyword. If you omit the **end** keyword, the rule is always in effect after the start time and date have passed.
Step 6	(Optional) [*sequence-number*] **absolute** [**start** *time date*] **end** *time date*	Creates an absolute rule that is in effect until the time and date specified after the **end** keyword. If you omit the **start**

	Command or Action	Purpose
	Example: `switch(config-time-range)# absolute end 23:59:59 31 december 2008`	keyword, the rule is always in effect until the end time and date have passed.
Step 7	(Optional) **no** {*sequence-number* | **periodic** *arguments* . . . | **absolute** *arguments*. . .} **Example:** `switch(config-time-range)# no 80`	Removes the specified rule from the time range.
Step 8	(Optional) **show time-range** *name* **Example:** `switch(config-time-range)# show time-range workday-daytime`	Displays the time-range configuration.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config-time-range)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Changing Sequence Numbers in a Time Range, on page 457

Removing a Time Range

You can remove a time range from the device.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command). Because ACL names can be repeated in different VDCs, we recommend that you confirm which VDC you are working in.

Ensure that you know whether the time range is used in any ACL rules. The device allows you to remove time ranges that are used in ACL rules. Removing a time range that is in use in an ACL rule does not affect the configuration of interfaces where you have applied the ACL. Instead, the device considers the ACL rule using the removed time range to be empty.

SUMMARY STEPS

1. **configure terminal**
2. **no time-range** *name*
3. (Optional) **show time-range**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no time-range** *name* **Example:** `switch(config)# no time-range daily-workhours`	Removes the time range that you specified by name.
Step 3	(Optional) **show time-range** **Example:** `switch(config-time-range)# show time-range`	Displays the configuration for all time ranges. The removed time range should not appear.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Changing Sequence Numbers in a Time Range

You can change all the sequence numbers assigned to rules in a time range.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command). Because ACL names can be repeated in different VDCs, we recommend that you confirm which VDC you are working in.

SUMMARY STEPS

1. **configure terminal**
2. **resequence time-range** *name starting-sequence-number increment*
3. (Optional) **show time-range** *name*
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**resequence time-range** *name starting-sequence-number increment* **Example:**	Assigns sequence numbers to the rules contained in the time range, where the first rule receives the starting sequence number that you specify. Each subsequent rule receives a

	Command or Action	Purpose
	`switch(config)# resequence time-range daily-workhours 100 10` `switch(config)#`	number larger than the preceding rule. The difference in numbers is determined by the increment that you specify.
Step 3	(Optional) **show time-range** *name* **Example:** `switch(config)# show time-range daily-workhours`	Displays the time-range 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.

Verifying the Time-Range Configuration

To display time-range configuration information, perform one of the following tasks. For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
show time-range	Displays the time-range configuration.
show running-config aclmgr	Displays ACL configuration, including all time ranges.

Additional References for IP ACLs

Related Documents

Related Topic	Document Title
IP ACL commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
Object group commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
Time range commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
SNMP	*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for IP ACLs

This table lists the release history for this feature.

Table 29: Feature History for IP ACLs

Feature Name	Releases	Feature Information
Configuring ACLs over M3 modules	7.3(0)DX(1)	Support for M3 modules is introduced.
Flexible ACL TCAM Bank Chaining	7.3(0)D1(1)	Added the support for the flexible ACL TCAM bank chaining feature.
ACL TCAM bank mapping	6.2(10)	Added a command to display the bank-mapping matrix.
IP ACLs	6.2(2)	Added support for ACL TCAM bank mapping.
IP ACLs	6.1(1)	Updated for M2 Series modules.
IP ACLs	6.0(1)	Updated for F2 Series modules.
FCoE ACLs	5.2(1)	Added support for FCoE ACLs on F1 Series modules.
IP ACLs	5.2(1)	Added support for ACL capture on M1 Series modules.
IP ACLs	5.2(1)	Changed the **show running-config aclmgr** and **show startup-config aclmgr** commands to display only the user-configured ACLs (and not also the default CoPP-configured ACLs) in the running and startup configurations.
VTY ACLs	5.1(1)	Added support to control access to traffic received over a VTY line.
IP ACLs	5.0(2)	Added support for up to 128K ACL entries when using an XL line card, provided a scalable services license is installed.
ACL logging	4.2(3)	Added support for logging of packets sent to the supervisor module for ACL processing.

Feature Name	Releases	Feature Information
IP ACLs	4.2(1)	Added support for MAC packet classification on Layer 2 interfaces.

CHAPTER 15

Configuring MAC ACLs

This chapter describes how to configure MAC access lists (ACLs) on Cisco NX-OS devices.

This chapter contains the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About MAC ACLs

MAC ACLs are ACLs that use information in the Layer 2 header of packets to filter traffic. MAC ACLs share many fundamental concepts with IP ACLs, including support for virtualization.

Related Topics

Information About ACLs, on page 406

MAC Packet Classification

MAC packet classification allows you to control whether a MAC ACL that is on a Layer 2 interface applies to all traffic entering the interface, including IP traffic, or to non-IP traffic only.

MAC packet classification does not work on the Layer 3 control plane protocols such as HSRP, VRRP, OSPF, and so on. If you enable MAC packet classification on the VLANs, the basic functionalities will break on these protocols.

MAC Packet Classification State	Effect on Interface
Enabled	• A MAC ACL that is on the interface applies to all traffic entering the interface, including IP traffic. • You cannot apply an IP port ACL on the interface.
Disabled	• A MAC ACL that is on the interface applies only to non-IP traffic entering the interface. • You can apply an IP port ACL on the interface.

Related Topics

Enabling or Disabling MAC Packet Classification, on page 468

Prerequisites for MAC ACLs

There are no prerequisites for configuring MAC ACLs.

Guidelines and Limitations for MAC ACLs

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.

Default Settings for MAC ACLs

This table lists the default settings for MAC ACL parameters.

Table 30: Default MAC ACLs Parameters

Parameters	Default
MAC ACLs	No MAC ACLs exist by default
ACL rules	Implicit rules apply to all ACLs

Configuring MAC ACLs

Creating a MAC ACL

You can create a MAC ACL and add rules to it.

SUMMARY STEPS

1. **configure terminal**
2. **mac access-list** *name*
3. {**permit** | **deny**} *source destination protocol*
4. (Optional) **statistics per-entry**
5. (Optional) **show mac access-lists** *name*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**mac access-list** *name*
	Example:
	`switch(config)# mac access-list acl-mac-01`
	`switch(config-mac-acl)#`
		Creates the MAC ACL and enters ACL configuration mode.

Step 3	{**permit** | **deny**} *source destination protocol* **Example:** `switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any`	Creates a rule in the MAC ACL. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.
Step 4	(Optional) **statistics per-entry** **Example:** `switch(config-mac-acl)# statistics per-entry`	Specifies that the device maintains global statistics for packets that match the rules in the ACL.
Step 5	(Optional) **show mac access-lists** *name* **Example:** `switch(config-mac-acl)# show mac access-lists acl-mac-01`	Displays the MAC ACL configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-mac-acl)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Changing a MAC ACL

You can remove a MAC ACL from the device.

Before you begin

Use the **show mac access-lists** command with the summary keyword to find the interfaces that a MAC ACL is configured on.

SUMMARY STEPS

1. **configure terminal**
2. **mac access-list** *name*
3. (Optional) [*sequence-number*] {**permit** | **deny**} *source destination protocol*
4. (Optional) **no** {*sequence-number* | {**permit** | **deny**} *source destination protocol*}
5. (Optional) [**no**] **statistics per-entry**
6. (Optional) **show mac access-lists** *name*
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**mac access-list** *name*
	Example:
	`switch(config)# mac access-list acl-mac-01`
	`switch(config-mac-acl)#`
		Enters ACL configuration mode for the ACL that you specify by name.

Step 3	(Optional) [*sequence-number*] {**permit** | **deny**} *source destination protocol* **Example:** `switch(config-mac-acl)# 100 permit mac 00c0.4f00.00 0000.00ff.ffff any`	Creates a rule in the MAC ACL. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the rules. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.
Step 4	(Optional) **no** {*sequence-number* | {**permit** | **deny**} *source destination protocol*} **Example:** `switch(config-mac-acl)# no 80`	Removes the rule that you specify from the MAC ACL. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.
Step 5	(Optional) [**no**] **statistics per-entry** **Example:**	Specifies that the device maintains global statistics for packets that match the rules in the ACL.

	Command or Action	Purpose
	`switch(config-mac-acl)# statistics per-entry`	The **no** option stops the device from maintaining global statistics for the ACL.
Step 6	(Optional) **show mac access-lists** *name* **Example:** `switch(config-mac-acl)# show mac access-lists acl-mac-01`	Displays the MAC ACL configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config-mac-acl)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

SUMMARY STEPS

1. **configure terminal**
2. **resequence mac access-list** *name starting-sequence-number increment*
3. (Optional) **show mac access-lists** *name*
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**resequence mac access-list** *name starting-sequence-number increment* **Example:** `switch(config)# resequence mac access-list acl-mac-01 100 10`	Assigns sequence numbers to the rules contained in the ACL, where the first rule receives the number specified by the starting-sequence number that you specify. Each subsequent rule receives a number larger than the preceding rule. The difference in numbers is determined by the increment number that you specify.
Step 3	(Optional) **show mac access-lists** *name* **Example:** `switch(config)# show mac access-lists acl-mac-01`	Displays the MAC ACL configuration.
Step 4	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

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

Removing a MAC ACL

You can remove a MAC ACL from the device.

SUMMARY STEPS

1. **configure terminal**
2. **no mac access-list** *name*
3. (Optional) **show mac access-lists** *name* **summary**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no mac access-list** *name*
	Example:
	`switch(config)# no mac access-list acl-mac-01`
	`switch(config)#`
		Removes the MAC ACL that you specify by name from the running configuration.

Step 3	(Optional) **show mac access-lists** *name* **summary** **Example:** `switch(config)# show mac access-lists acl-mac-01 summary`	Displays the MAC ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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:

- Layer 2 or Layer 3 Ethernet interfaces
- Layer 2 or Layer 3 port-channel interfaces

Before you begin

Ensure that the ACL that you want to apply exists and is configured to filter traffic in the manner that you need for this application.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
   - **interface ethernet** *slot*/*port*
   - **interface port-channel** *channel-number*
3. **mac port access-group** *access-list*
4. (Optional) **show running-config aclmgr**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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)#`
	Example:
	`switch(config)# interface port-channel 5`
	`switch(config-if)#`
		• Enters interface configuration mode for a Layer 2 or Layer 3 interface.
		• Enters interface configuration mode for a Layer 2 or Layer 3 port-channel interface.

Step 3	**mac port access-group** *access-list* **Example:** `switch(config-if)# mac port access-group acl-01`	Applies a MAC ACL to the interface.
Step 4	(Optional) **show running-config aclmgr** **Example:** `switch(config-if)# show running-config aclmgr`	Displays ACL configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Applying a MAC ACL as a VACL

You can apply a MAC ACL as a VACL.

Related Topics

Configuring VACLs, on page 476

Enabling or Disabling MAC Packet Classification

You can enable or disable MAC packet classification on a Layer 2 interface.

Before you begin

The interface must be configured as a Layer 2 interface. Note that the M1 and M2 Series modules do not support IP ACLs on port ACL and VACL policies, when the MAC packet classification feature is enabled on the interface. Before you upgrade to Cisco NX-OS Release 6.x or later versions, you need to disable the MAC packet classification feature on M1 and M2 Series modules, and verify whether all the existing functionalities work.

Note If the interface is configured with the **ip port access-group** command or the **ipv6 port traffic-filter** command, you cannot enable MAC packet classification until you remove the **ip port access-group** and **ipv6 port traffic-filter** commands from the interface configuration.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
    - **interface ethernet** *slot/port*
    - **interface port-channel** *channel-number*
3. [**no**] **mac packet-classify**
4. (Optional) Enter one of the following commands:
    - **show running-config interface ethernet** *slot/port*
    - **show running-config interface port-channel** *channel-number*
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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*	• Enters interface configuration mode for a Ethernet interface.

	Command or Action	Purpose

	• **interface port-channel** *channel-number*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
	Example:
	`switch(config)# interface port-channel 5`
	`switch(config-if)#`
		• Enters interface configuration mode for a port-channel interface.

Step 3	[**no**] **mac packet-classify** **Example:** `switch(config-if)# mac packet-classify`	Enables MAC packet classification on the interface. The **no** option disables MAC packet classification on the interface.

Step 4	(Optional) Enter one of the following commands:
	• **show running-config interface ethernet** *slot/port*
	• **show running-config interface port-channel** *channel-number*
	Example:
	`switch(config-if)# show running-config interface ethernet 2/1`
	Example:
	`switch(config-if)# show running-config interface port-channel 5`
		• Displays the running configuration of the Ethernet interface.
		• Displays the running configuration of the port-channel interface.

Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

MAC Packet Classification, on page 462

Verifying the MAC ACL Configuration

To display MAC ACL configuration information, perform one of the following tasks. For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
show mac access-lists	Displays the MAC ACL configuration.

Command	Purpose
show running-config aclmgr [**all**]	Displays the ACL configuration, including MAC ACLs and the interfaces to which MAC ACLs are applied. **Note** Beginning with Cisco NX-OS Release 5.2, this command displays the user-configured ACLs in the running configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
show startup-config aclmgr [**all**]	Displays the ACL startup configuration. **Note** Beginning with Cisco NX-OS Release 5.2, this command displays the user-configured ACLs in the startup configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

Monitoring and Clearing MAC ACL Statistics

Use the **show mac access-lists** command to monitor statistics about a MAC ACL, including the number of packets that have matched each rule.

To monitor or clear MAC ACL statistics, use one of the commands in this table. For detailed information about these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
show mac access-lists	Displays the MAC ACL configuration. If the MAC ACL includes the statistics per-entry command, the **show mac access-lists** command output includes the number of packets that have matched each rule.
clear mac access-list counters	Clears statistics for all MAC ACLs or for a specific MAC ACL.

Configuration Example for MAC ACLs

The following example shows how to create a MAC ACL named acl-mac-01 and apply it to Ethernet interface 2/1, which is a Layer 2 interface in this example:

```
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any
interface ethernet 2/1
  mac port access-group acl-mac-01
```

Additional References for MAC ACLs

Related Documents

Related Topic	Document Title
MAC ACL commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for MAC ACLs

This table lists the release history for this feature.

Table 31: Feature History for MAC ACLs

Feature Name	Releases	Feature Information
MAC ACLs	6.1(1)	Updated for M2 Series modules.
MAC ACLs	6.0(1)	Updated for F2 Series modules.
MAC ACLs	5.2(1)	Changed the **show running-config aclmgr** and **show startup-config aclmgr** commands to display only the user-configured ACLs (and not also the default CoPP-configured ACLs) in the running and startup configurations.
MAC ACLs	5.0(2)	Support was added for up to 128,000 ACL entries when using an XL line card, provided a scalable services license is installed.

Feature Name	Releases	Feature Information
MAC ACLs	4.2(1)	Support was added for MAC packet classification.

CHAPTER 16

Configuring VLAN ACLs

This chapter describes how to configure VLAN access lists (ACLs) on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About VLAN ACLs

A VLAN ACL (VACL) is one application of an IP ACL or a MAC ACL. You can configure VACLs to apply to all packets that are routed into or out of a VLAN or are bridged within a VLAN. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VACLs are not defined by direction (ingress or egress).

Related Topics

Information About ACLs, on page 406

VLAN Access Maps and Entries

VACLs use access maps to contain an ordered list of one or more map entries. Each map entry associates IP or MAC ACLs to an action. Each entry has a sequence number, which allows you to control the precedence of entries.

When the device applies a VACL to a packet, it applies the action that is configured in the first access map entry that contains an ACL that permits the packet.

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 the normal operation of the switch.

Redirect

Redirects the traffic to one or more specified interfaces.

Drop

Drops the traffic. If you specify drop as the action, you can also specify that the device logs the dropped packets.

VACL Statistics

The 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 device does not support interface-level VACL statistics.

For each VLAN access map that you configure, you can specify whether the device maintains statistics for that VACL. This feature 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.

Related Topics

Monitoring and Clearing VACL Statistics, on page 481

Session Manager Support for VACLs

Session Manager supports the configuration of VACLs. 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. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.

Virtualization Support for VACLs

The following information applies to VACLs used in virtual device contexts (VDCs):

- ACLs are unique per VDC. You cannot use an ACL that you created in one VDC in a different VDC.
- Because ACLs are not shared by VDCs, you can reuse ACL names in different VDCs.
- The device does not limit ACLs or rules on a per-VDC basis.

Licensing Requirements for VACLs

This table shows the licensing requirements for this feature.

Product	License Requirement
Cisco NX-OS	VACLs require no license. However to support up to 128,000 ACL entries using an XL line card, you must install the scalable services 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 an explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Prerequisites for VACLs

VACLs have the following prerequisite:

- Ensure that the IP ACL or MAC 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 VACLs

VACLs have the following configuration guidelines:

- 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. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*.
- ACL statistics are not supported if the DHCP snooping feature is enabled. However, ACL statistics are supported on F3 and M3 Series modules if the DHCP snooping feature is enabled.
- The maximum number of supported VACL entries is 64,000 for devices without an XL line card and 128,000 for devices with an XL line card.
- If you try to apply too many ACL entries to a non-XL line card, the configuration is rejected.
- Each forwarding engine on an F1 Series module supports 1000 ingress ACL entries, with 984 entries available for user configuration. The total number of VACL entries for the F1 Series modules is from 1000 to 16,000, depending on which forwarding engines the policies are applied.
- Each of the 16 forwarding engines in an F1 Series module supports up to 250 IPv6 addresses across multiple ACLs.
- F1 Series modules do not support ACL logging.

- F1 Series modules do not support bank chaining.
- Each VACL can support up to six different Layer 4 operations for F1 Series modules.
- If the same ACL is applied on multiple VLANs of the same port for F1 Series modules (for example, VLAN 10, 20), it is programmed multiple times (in this case, on VLAN 10 and VLAN 20).
- Each of the 12 forwarding engines in an F2 Series module has 16,000 total TCAM entries, equally split across two banks. 168 default entries are reserved. Each forwarding engine also has 512 IPv6 compression TCAM entries.
- Each of the 12 forwarding engines in an F3 Series module has 16,000 total TCAM entries, equally split across four TCAM banks, that is, T0B0, T0B1, T1B0, and T1B1.
- Each of the 6 forwarding engines in an M3 Series module has 128,000 total TCAM entries, equally split across four TCAM banks, that is, T0B0, T0B1, T1B0, and T1B1.
- VACL redirects to SPAN destination ports are not supported. This guideline is also applicable for M3 and F3 Series modules.
- Only F2 Series, F3 Series, M1 Series, M2 Series, and M3 Series modules support deny ACEs in a sequence.
- Statistics for deny ACE support are supported only for the terminating sequence for the following sequence-based features: VACL, policy-based routing (PBR), and quality of service (QoS). This guideline is also applicable for M3 and F3 Series modules.

Default Settings for VACLs

This table lists the default settings for VACL parameters.

Table 32: Default VACL Parameters

Parameters	Default
VACLs	No IP ACLs exist by default
ACL rules	Implicit rules apply to all ACLs
Deny ACE support	Disabled

Configuring VACLs

Creating a VACL or Adding a VACL Entry

You can create a VACL or add entries to an existing VACL. In both cases, you create a VACL entry, which is a VLAN access-map entry that associates one or more ACLs with an action to be applied to the matching traffic.

Before you begin

Ensure that the ACLs that you want to use in the VACL exists and are configured to filter traffic in the manner that you need for this application.

SUMMARY STEPS

1. **configure terminal**
2. **vlan access-map** *map-name* [*sequence-number*]
3. Enter one of the following commands:
   - **match** {**ip** | **ipv6**} **address** *ip-access-list*
   - **match mac address** *mac-access-list*
4. **action** {**drop** | **forward** | **redirect**}
5. (Optional) [**no**] **statistics per-entry**
6. (Optional) **show running-config aclmgr**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**vlan access-map** *map-name* [*sequence-number*]
	Example:
	`switch(config)# vlan access-map acl-mac-map`
	`switch(config-access-map)#`
		Enters VLAN access-map configuration mode for the VLAN access map specified. If the VLAN access map does not exist, the device creates it.
		If you do not specify a sequence number, the device creates a new entry whose sequence number is 10 greater than the last sequence number in the access map.

Step 3	Enter one of the following commands:
	• **match** {**ip** | **ipv6**} **address** *ip-access-list*
	• **match mac address** *mac-access-list*
	Example:
	`switch(config-access-map)# match mac address acl-ip-lab`
	Example:
	`switch(config-access-map)# match mac address acl-mac-01`
		Specifies an ACL for the access-map entry.

Step 4	**action** {**drop** | **forward** | **redirect**} **Example:** `switch(config-access-map)# action forward`	Specifies the action that the device applies to traffic that matches the ACL. The **action** command supports many options. For more information, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

	Command or Action	Purpose
Step 5	(Optional) [**no**] **statistics per-entry** **Example:** `switch(config-access-map)# statistics per-entry`	Specifies that the device maintains global statistics for packets that match the rules in the VACL. The **no** option stops the device from maintaining global statistics for the VACL.
Step 6	(Optional) **show running-config aclmgr** **Example:** `switch(config-access-map)# show running-config aclmgr`	Displays the ACL configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config-access-map)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Removing a VACL or a VACL Entry

You can remove a VACL, which means that you will delete the VLAN access map.

You can also remove a single VLAN access-map entry from a VACL.

Before you begin

Ensure that you know whether the VACL is applied to a VLAN. The device 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 device considers the removed VACL to be empty.

SUMMARY STEPS

1. **configure terminal**
2. **no vlan access-map** *map-name* [*sequence-number*]
3. (Optional) **show running-config aclmgr**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no vlan access-map** *map-name* [*sequence-number*] **Example:** `switch(config)# no vlan access-map acl-mac-map 10`	Removes the VLAN access map configuration for the specified access map. If you specify the *sequence-number* argument and the VACL contains more than one entry, the command removes only the entry specified.

	Command or Action	Purpose
Step 3	(Optional) **show running-config aclmgr** **Example:** `switch(config)# show running-config aclmgr`	Displays the ACL 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.

Applying a VACL to a VLAN

You can apply a VACL to a VLAN.

Before you begin

If you are applying a VACL, ensure that the VACL exists and is configured to filter traffic in the manner that you need for this application.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **vlan filter** *map-name* **vlan-list** *list*
3. (Optional) **show running-config aclmgr**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **vlan filter** *map-name* **vlan-list** *list*
	Example:
	`switch(config)# vlan filter acl-mac-map vlan-list 1-20,26-30`
	`switch(config)#`
		Applies the VACL to the VLANs by the list that you specified. The **no** option unapplies the VACL.

Step 3	(Optional) **show running-config aclmgr** **Example:** `switch(config)# show running-config aclmgr`	Displays the ACL 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 Deny ACE Support

You can configure the device to support deny access control entries (ACEs) in a sequence for the following sequence-based features: VACL, policy-based routing (PBR), and QoS. When deny ACEs are enabled, the traffic that matches a **deny** ACE (an ACL rule with the deny keyword) in a class-map-acl is recursively matched against subsequent class-map-acls until it hits a permit ACE.

Before you begin

Ensure that you are in the default or admin VDC.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **hardware access-list allow deny ace**
3. (Optional) **show running-config aclmgr**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **hardware access-list allow deny ace** **Example:** `switch(config)# hardware access-list allow deny ace`	Enables support for deny ACEs in a sequence.
Step 3	(Optional) **show running-config aclmgr** **Example:** `switch(config)# show running-config aclmgr`	Displays the ACL 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.

Verifying the VACL Configuration

To display VACL configuration information, perform one of the following tasks. For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
show running-config aclmgr [**all**]	Displays the ACL configuration, including the VACL-related configuration. **Note** Beginning with Cisco NX-OS Release 5.2, this command displays the user-configured ACLs in the running configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
show startup-config aclmgr [**all**]	Displays the ACL startup configuration. **Note** Beginning with Cisco NX-OS Release 5.2, this command displays the user-configured ACLs in the startup configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.
show vlan filter	Displays information about VACLs that are applied to a VLAN.
show vlan access-map	Displays information about VLAN access maps.

Monitoring and Clearing VACL Statistics

To monitor or clear VACL statistics, use one of the commands in this table. For detailed information about these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
show vlan access-list	Displays the VACL configuration. If the VLAN access-map includes the **statistics per-entry** command, the **show vlan access-list** command output includes the number of packets that have matched each rule.
clear vlan access-list counters	Clears statistics for all VACLs or for a specific VACL.

Configuration Example for VACLs

The following example shows how to configure a VACL to forward traffic permitted by a MAC ACL named acl-mac-01 and how to apply the VACL to VLANs 50 through 82.

```
conf t
vlan access-map acl-mac-map
```

```
  match mac address acl-mac-01
  action forward
vlan filter acl-mac-map vlan-list 50-82
```

Additional References for VACLs

Related Documents

Related Topic	Document Title
VACL commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
Policy-based routing (PBR) configuration	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*
QoS configuration	*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for VLAN ACLs

This table lists the release history for this feature.

Table 33: Feature History for VLAN ACLs

Feature Name	Releases	Feature Information
VLAN ACLs	6.1(3)	Added support for deny ACEs in a sequence.
VLAN ACLs	6.0(1)	Updated for F2 Series modules.

Feature Name	Releases	Feature Information
VLAN ACLs	5.2(1)	Changed the **show running-config aclmgr** and **show startup-config aclmgr** commands to display only the user-configured ACLs (and not also the default CoPP-configured ACLs) in the running and startup configurations.
VLAN ACLs	5.1(1)	No change from Release 5.0.
VLAN ACLs	5.0(2)	Added support for up to 128,000 ACL entries when using an XL line card, provided a scalable services license is installed.
VLAN access maps	4.2(1)	No change from Release 4.1.

CHAPTER 17

Configuring Port Security

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

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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 interfacesphysical 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.

Related Topics

Secure MAC Address Maximums, on page 487

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.

Related Topics

Removing a Static Secure MAC Address on an Interface, on page 500
Port Type Changes, on page 492

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 in the configuration of 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.
- You configure the interface to act as a Layer 3 interface.

Related Topics

Dynamic Address Aging, on page 487
Removing a Dynamic Secure MAC Address, on page 502

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 in the configuration of an interface until one of the following events occurs:

- You explicitly remove the address.
- You configure the interface to act as a Layer 3 interface.

Related Topics

Removing a Sticky Secure MAC Address, on page 501

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.

Related Topics

Security Violations and Actions, on page 488
Removing a Dynamic Secure MAC Address, on page 502
Removing a Sticky Secure MAC Address, on page 501
Removing a Static Secure MAC Address on an Interface, on page 500

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 10 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.
- The device has learned 10 addresses on the interface and inbound traffic from an 11th address arrives at the interface.

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 pscecure-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

Note If an interface is errDisabled, you can bring it up only by flapping the interface.

Port Security and Port Types

You can configure port security only on Layer 2 interfaces. Details about port security and different types of interfaces or ports are as follows:

Access ports

You can configure port security on interfaces that you have configured as Layer 2 access ports. On an access port, port security applies only to the access VLAN. VLAN maximums are not useful for access ports.

Trunk ports

You can configure port security on interfaces that you have configured as Layer 2 trunk ports. The device allows VLAN maximums only for VLANs associated with the trunk port.

SPAN ports

You can configure port security on SPAN source ports but not on SPAN destination ports.

Ethernet port channels

You can configure port security on Layer 2 Ethernet port channels in either access mode or trunk mode.

Fabric Extender (FEX) ports

Port security is supported on GEM and FEX ports.

Private VLAN Enabled Ports

Port Security is supported on ports that are enabled as Private VLAN ports.

PVLAN Host (physical interfaces only)

You can configure Private VLANs (PVLANs) to provide traffic separation and security at the Layer 2 level. A PVLAN is one or more pairs of a primary VLAN and a secondary VLAN, all with the same primary VLAN.

PVLAN Promiscuous (physical interfaces only)

You can configure a Layer 2 VLAN network interface, or switched virtual interface (SVI), on the PVLAN promiscuous port, which provides routing functionality to the primary PVLAN. This is supported on physical interfaces only.

PVLAN trunk secondary/promiscuous

You can configure PVLAN trunk secondary/promiscuous in the of switchport mode. This is supported for both physical interface and portchannel.

Port Security and Port-Channel Interfaces

Port security is supported on Layer 2 port-channel interfaces. Port security operates on port-channel interfaces in the same manner as on physical interfaces, except as described in this section.

General guidelines

Port security on a port-channel interface operates in either access mode or trunk mode. In trunk mode, the MAC address restrictions enforced by port security apply to all member ports on a per-VLAN basis.

Enabling port security on a port-channel interface does not affect port-channel load balancing.

Port security does not apply to port-channel control traffic passing through the port-channel interface. Port security allows port-channel control packets to pass without causing security violations. Port-channel control traffic includes the following protocols:

- Port Aggregation Protocol (PAgP)
- Link Aggregation Control Protocol (LACP)
- Inter-Switch Link (ISL)
- IEEE 802.1Q

Configuring secure member ports

The port security configuration of a port-channel interface has no effect on the port security configuration of member ports.

Adding a member port

If you add a secure interface as a member port of a port-channel interface, the device discards all dynamic secure addresses learned on the member port but retains all other port-security configuration of the member port in the running configuration. Sticky and static secure MAC addresses learned on the secure member port are also stored in the running configuration rather than NVRAM.

If port security is enabled on the member port and not enabled on the port-channel interface, the device warns you when you attempt to add the member port to the port-channel interface. You can use the **force** keyword with the **channel-group** command to forcibly add a secure member port to a nonsecure port-channel interface.

While a port is a member of a port-channel interface, you cannot configure port security on the member port. To do so, you must first remove the member port from the port-channel interface.

Removing a member port

If you remove a member port from a port-channel interface, the device restores the port security configuration of the member port. Static and sticky secure MAC addresses that were learned on the port before you added it to the port-channel interface are restored to NVRAM and removed from the running configuration.

Note To ensure that all ports are secure as needed after you remove a port-channel interface, we recommend that you closely inspect the port-security configuration of all member ports.

Removing a port-channel interface

If you remove a secure port-channel interface, the following occurs:

- The device discards all secure MAC addresses learned for the port-channel interface, including static and sticky secure MAC addresses learned on the port-channel interface.
- The device restores the port-security configuration of each member port. The static and sticky secure MAC addresses that were learned on member ports before you added them to the port-channel interface are restored to NVRAM and removed from the running configuration. If a member port did not have port security enabled prior to joining the port-channel interface, port security is not enabled on the member port after the port-channel interface is removed.

Note To ensure that all ports are secure as needed after you remove a port-channel interface, we recommend that you closely inspect the port-security configuration of all member ports.

Disabling port security

If port security is enabled on any member port, the device does not allow you to disable port security on the port-channel interface. To do so, remove all secure member ports from the port-channel interface first. After disabling port security on a member port, you can add it to the port-channel interface again, as needed.

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.

When you change a Layer 2 interface from an access port to a trunk port, the device drops all secure addresses learned by the dynamic method. The device moves the addresses learned by the static method to the native trunk VLAN. If VLAN already exists, the sticky MACs remain in same VLAN otherwise they move to 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

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 addressees 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.

Virtualization Support for Port Security

Port security supports VDCs as follows:

- Port security is local to each VDC. You enable and configure port security on a per-VDC basis.
- Each VDC maintains secure MAC addresses separately.
- The device cannot issue a security violation when a secured MAC address in one VDC is seen on a protected interface in another VDC.

Prerequisites for Port Security

Port security has the following prerequisites:

- You must globally enable port security for the device that you want to protect with port security.

Default Settings for Port Security

This table lists the default settings for port security parameters.

Table 34: Default Port Security Parameters

Parameters	Default
Port security enablement globally	Disabled
Port security enablement per interface	Disabled
MAC address learning method	Dynamic
Interface maximum number of secure MAC addresses	1
Security violation action	Shutdown
Aging type	Absolute
Aging time	0

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.
- Port security is not supported on vPC ports.
- Port security operates with 802.1X on Layer 2 Ethernet interfaces.

Related Topics

802.1X and Port Security, on page 268

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.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **feature port-security**
3. **show port-security**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **feature port-security** **Example:** `switch(config)# feature port-security`	Enables port security globally. The **no** option disables port security globally.

	Command or Action	Purpose
Step 3	**show port-security** **Example:** `switch(config)# show port-security`	Displays the status of port security.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

When you disable port security on an interface, all switchport port security configuration for the interface is lost.

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.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
    - **interface ethernet** *slot*/*port*
    - **interface port-channel** *channel-number*
3. **switchport**
4. [**no**] **switchport port-security**
5. **show running-config port-security**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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 for the Ethernet or port-channel interface that you want to configure with port security.

Step 3	**switchport** **Example:** `switch(config-if)# switchport`	Configures the interface as a Layer 2 interface.
Step 4	[**no**] **switchport port-security** **Example:** `switch(config-if)# switchport port-security`	Enables port security on the interface. The **no** option disables port security on the interface.

Step 5	**show running-config port-security**
	Example:
	`switch(config-if)# show running-config`
	`port-security`
		Displays the port security configuration.

Step 6	(Optional) **copy running-config startup-config**
	Example:
	`switch(config-if)# copy running-config`
	`startup-config`
		Copies the running configuration to the startup configuration.

Related Topics

Secure MAC Address Learning, on page 486
Enabling or Disabling Sticky MAC Address Learning, on page 497

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.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
   - **interface ethernet** *slot*/*port*
   - **interface port-channel** *channel-number*
3. **switchport**
4. [**no**] **switchport port-security mac-address sticky**
5. **show running-config port-security**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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 for the interface that you want to configure with sticky MAC address learning.

Step 3	**switchport** **Example:** `switch(config-if)# switchport`	Configures the interface as a Layer 2 interface.
Step 4	[**no**] **switchport port-security mac-address sticky** **Example:** `switch(config-if)# switchport port-security mac-address sticky`	Enables sticky MAC address learning on the interface. The **no** option disables sticky MAC address learning.
Step 5	**show running-config port-security** **Example:** `switch(config-if)# show running-config port-security`	Displays the port security configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
    - **interface ethernet** *slot*/*port*
    - **interface port-channel** *channel-number*
3. [**no**] **switchport port-security mac-address** *address* [**vlan** *vlan-ID*]
4. **show running-config port-security**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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 for the interface that you specify.

Step 3	[**no**] **switchport port-security mac-address** *address* [**vlan** *vlan-ID*] **Example:** `switch(config-if)# switchport port-security mac-address 0019.D2D0.00AE`	Configures a static MAC address for port security on the current interface. Use the **vlan** keyword if you want to specify the VLAN that traffic from the address is allowed on.

	Command or Action	Purpose
Step 4	**show running-config port-security** **Example:** `switch(config-if)# show running-config port-security`	Displays the port security configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Verifying the Port Security Configuration, on page 507
Configuring a Maximum Number of MAC Addresses, on page 503
Removing a Dynamic Secure MAC Address, on page 502
Removing a Static Secure MAC Address on an Interface, on page 500

Removing a Static Secure MAC Address on an Interface

You can remove a static secure MAC address on a Layer 2 interface.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
   - **interface ethernet** *slot*/*port*
   - **interface port-channel** *channel-number*
3. **no switchport port-security mac-address** *address*
4. **show running-config port-security**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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 for the interface from which you want to remove a static secure MAC address.

	Command or Action	Purpose
Step 3	**no switchport port-security mac-address** *address* **Example:** `switch(config-if)# no switchport port-security mac-address 0019.D2D0.00AE`	Removes the static secure MAC address from port security on the current interface.
Step 4	**show running-config port-security** **Example:** `switch(config-if)# show running-config port-security`	Displays the port security configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
   - **interface ethernet** *slot*/*port*
   - **interface port-channel** *channel-number*
3. **no switchport port-security mac-address sticky**
4. **clear port-security dynamic address** *address*
5. (Optional) **show port-security address interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*}
6. (Optional) **switchport port-security mac-address sticky**

DETAILED STEPS

	Command or Action	Purpose

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*	Enters interface configuration mode for the interface from which you want to remove a sticky secure MAC address.

	Command or Action	Purpose

	• **interface port-channel** *channel-number*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`	

Step 3	**no switchport port-security mac-address sticky** **Example:** `switch(config-if)# no switchport port-security mac-address sticky`	Disables sticky MAC address learning on the interface, which converts any sticky secure MAC addresses on the interface to dynamic secure MAC addresses.
Step 4	**clear port-security dynamic address** *address* **Example:** `switch(config-if)# clear port-security dynamic address 0019.D2D0.02GD`	Removes the dynamic secure MAC address that you specify.
Step 5	(Optional) **show port-security address interface** {**ethernet** *slot/port* | **port-channel** *channel-number*} **Example:** `switch(config)# show port-security address`	Displays secure MAC addresses. The address that you removed should not appear.
Step 6	(Optional) **switchport port-security mac-address sticky** **Example:** `switch(config-if)# switchport port-security mac-address sticky`	Enables sticky MAC address learning again on the interface.

Removing a Dynamic Secure MAC Address

You can remove dynamically learned, secure MAC addresses.

Before you begin

You must have enabled port security globally.

SUMMARY STEPS

1. **configure terminal**
2. **clear port-security dynamic** {**interface ethernet** *slot*/*port* | **address** *address*} [**vlan** *vlan-ID*]
3. **show port-security address**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
Step 2	**clear port-security dynamic** {**interface ethernet** *slot*/*port* | **address** *address*} [**vlan** *vlan-ID*] **Example:** `switch(config)# clear port-security dynamic interface ethernet 2/1`	Removes dynamically learned, secure MAC addresses, as specified. 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.
Step 3	**show port-security address** **Example:** `switch(config)# show port-security address`	Displays secure MAC addresses.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	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.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:

- **interface ethernet** *slot*/*port*
- **interface port-channel** *channel-number*

3. [**no**] **switchport port-security maximum** *number* [**vlan** *vlan-ID*]
4. **show running-config port-security**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Removing a Dynamic Secure MAC Address, on page 502
Removing a Static Secure MAC Address on an Interface, on page 500

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.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
   - **interface ethernet** *slot*/*port*
   - **interface port-channel** *channel-number*
3. [**no**] **switchport port-security aging type** {**absolute** | **inactivity**}
4. [**no**] **switchport port-security aging time** *minutes*
5. **show running-config port-security**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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 for the interface that you want to configure with the MAC aging type and time.

Step 3	[**no**] **switchport port-security aging type** {**absolute** | **inactivity**} **Example:** `switch(config-if)# switchport port-security aging type inactivity`	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. **Note** F1 series modules do not support the **inactivity** aging type.
Step 4	[**no**] **switchport port-security aging time** *minutes* **Example:**	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**

	Command or Action	Purpose
	`switch(config-if)# switchport port-security aging time 120`	option resets the aging time to the default, which is 0 minutes (no aging).
Step 5	**show running-config port-security** **Example:** `switch(config-if)# show running-config port-security`	Displays the port security configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
   - **interface ethernet** *slot*/*port*
   - **interface port-channel** *channel-number*
3. [**no**] **switchport port-security violation** {**protect** | **restrict** | **shutdown**}
4. **show running-config port-security**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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*	Enters interface configuration mode for the interface that you want to configure with a security violation action.

	Command or Action	Purpose

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

Step 3	[**no**] **switchport port-security violation** {**protect** | **restrict** | **shutdown**} **Example:** `switch(config-if)# switchport port-security violation restrict`	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.
Step 4	**show running-config port-security** **Example:** `switch(config-if)# show running-config port-security`	Displays the port security configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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*.

Command	Purpose
show running-config port-security	Displays the port security configuration.
show port-security	Displays the port security status of the device.
show port-security interface	Displays the port security status of a specific interface.
show port-security address	Displays secure MAC addresses.

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 *Cisco Nexus 7000 Series NX-OS Security Command Reference*

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
```

Feature History for Port Security

This table lists the release history for this feature.

Table 35: Feature History for Port Security

Feature Name	Releases	Feature Information	
Port security	6.0(1)	No change from Release 5.2.	
Port security	5.2(1)	No change from Release 5.1.	
Port security	5.1(1)	No change from Release 5.0.	
Port security	5.0(2)	No change from Release 4.2.	
Port security	4.2(1)	Support for Layer 2 port-channel interfaces was added.	

CHAPTER 18

Configuring DHCP

This chapter describes how to configure the Dynamic Host Configuration Protocol (DHCP) on a Cisco NX-OS device.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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 can be enabled globally and on a per-VLAN basis. By default, the feature is disabled globally and on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

Trusted and Untrusted Sources

You can configure whether DHCP snooping trusts traffic sources. An untrusted source may 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 device that is under your administrative control. These devices include the switches, routers, and servers in the network. Any device 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 device that is not in the service provider network is an untrusted source (such as a customer switch). Host ports are untrusted sources.

In the Cisco NX-OS 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 devices (such as switches or routers) inside your network. You usually do not configure host port interfaces as trusted.

Note For DHCP snooping to function properly, all DHCP servers must be connected to the device 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 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 device receives specific DHCP messages. For example, the feature adds an entry to the database when the device receives a DHCPACK message from the server. The feature removes the entry in the database when the IP address lease expires or the device 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.

Dynamic ARP inspection (DAI) and IP Source Guard also use information stored in the DHCP snooping binding database.

You can remove entries from the binding database by using the **clear ip dhcp snooping binding** command.

Related Topics

Clearing the DHCP Snooping Binding Database, on page 546

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 device. The third device can be a switch, server, or any other networking device 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. As a result, DHCP snooping and associated features such as dynamic ARP inspection (DAI) and IP Source Guard are disrupted. Beginning with Cisco NX-OS Release 5.1, 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 synchronized in the following scenarios:

- When the remote vPC is online, all the binding entries for that vPC link should be synchronized with the peer.
- When DHCP snooping is enabled on the peer switch, the dynamic binding entries for all vPC links should be synchronized with the peer.

Packet Validation

The device validates DHCP packets received on the untrusted interfaces of VLANs that have DHCP snooping enabled. The device forwards the DHCP packet unless any of the following conditions occur (in which case, the packet is dropped):

- The device receives a DHCP response packet (such as a DHCPACK, DHCPNAK, or DHCPOFFER packet) on an untrusted interface.

- The device 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 device 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.

Related Topics

Enabling or Disabling Strict DHCP Packet Validation, on page 525

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.

   Note For vPC peer switches, the remote ID suboption contains the vPC switch MAC address, which is unique in both switches. This MAC address is computed with the vPC domain ID. The Option 82 information is inserted at the switch where the DHCP request is first received before it is forwarded to the other vPC peer switch.

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. The 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 21: 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.

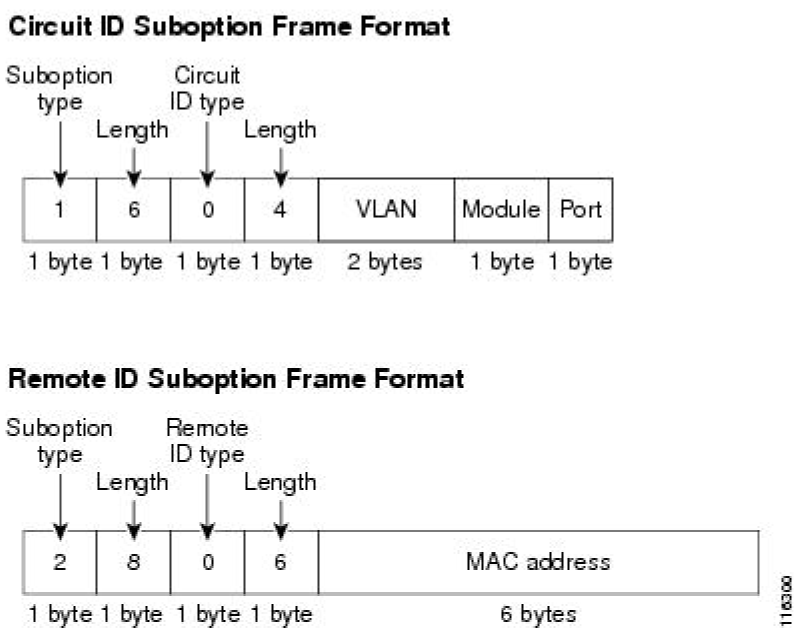
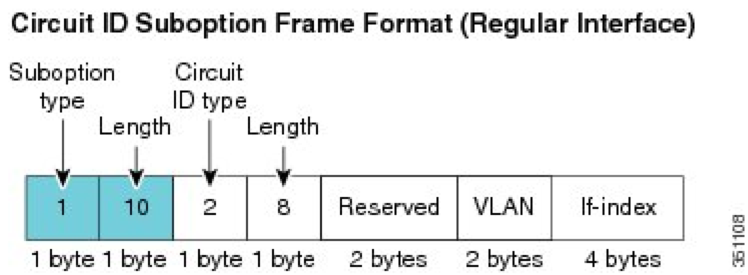
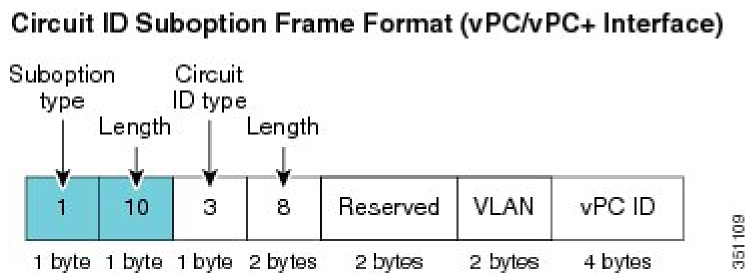


Figure 22: Circuit ID Suboption Frame Format for Regular and vPC Interfaces

Beginning with Cisco NX-OS Release 6.2(2), a new circuit ID format is used when Option 82 is enabled in DHCP snooping. The new circuit ID format is used by default and cannot be disabled. However, you might need to configure the DHCP server for the new circuit ID format if it was using the old Option 82 format for IP address allocation. These figures show the new default circuit ID format that is used for regular interfaces and vPC interfaces when Option 82 is enabled for DHCP snooping.

The enhanced Option 82 format improves DHCP packet processing. For vPC and vPC+ interfaces, the new format assigns vPC peers a unique circuit ID in case some are configured with different port channel numbers.





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.

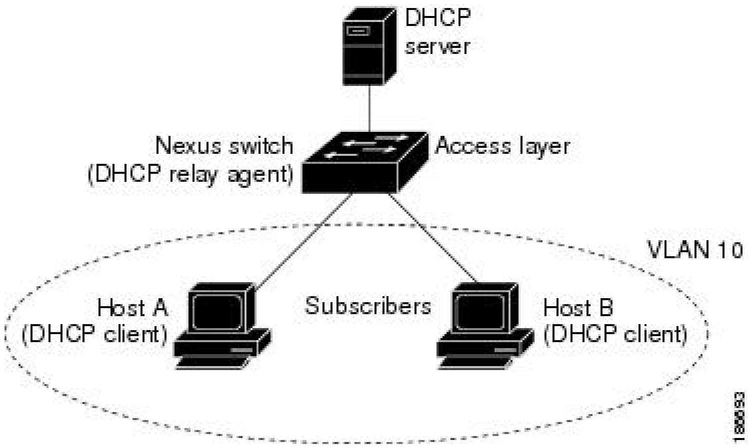
Note When the device relays a DHCP request that already includes Option 82 information, the device forwards the request with the original Option 82 information without altering it.

DHCP Relay Agent Option 82

You can enable the device to insert and remove Option 82 information on DHCP packets that are forwarded by the relay agent.

Figure 23: DHCP Relay Agent in a Metropolitan Ethernet Network

This figure shows an example of a metropolitan Ethernet network in which a centralized DHCP server assigns IP addresses to subscribers connected to the device at the access layer. Because the DHCP clients and their associated DHCP server do not reside on the same IP network or subnet, a DHCP relay agent is configured with a helper address to enable broadcast forwarding and to transfer DHCP messages between the clients and the server.



When you enable Option 82 for the DHCP relay agent 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). In DHCP relay, the circuit ID is filled with the if_index of the SVI or Layer 3 interface on which DHCP relay is configured.

Note For vPC peer devices, the remote ID suboption contains the vPC device MAC address, which is unique in both devices. This MAC address is computed with the vPC domain ID. The Option 82 information is inserted at the device where the DHCP request is first received before it is forwarded to the other vPC peer device.

3. When **dhcp relay source interface** *interface* is configured the device adds the configured source interface IP address as giaddr to the DHCP packet if source interface vrf is same as that of DHCP server VRF, otherwise IP address of the interface through which the server is reachable will be used as giaddr.
4. The device forwards the DHCP request that includes the Option 82 field to the DHCP server.
5. 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.
6. The DHCP server unicasts the reply to the Cisco NX-OS device if the request was relayed to the server by the 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. The 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.

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. For general information about VRFs, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

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 DCHP 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. When DHCP smart relay is enabled, the link selection is filled with the subnet of the active giaddr.

Server identifier override

IP address of the interface that receives the DHCP request. When DHCP smart relay is enabled, the server identifier is filled with the active giaddr.

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.

Related Topics

Enabling or Disabling VRF Support for the DHCP Relay Agent, on page 535

DHCP Smart Relay Agent

When the DHCP relay agent receives broadcast DHCP request packets from a host, it sets giaddr to the primary address of the inbound interface and forwards the packets to the server. The server allocates IP addresses from the giaddr subnet pool until the pool is exhausted and ignores further requests.

Beginning with Cisco NX-OS Release 5.2, you can configure the DHCP smart relay agent to allocate IP addresses from the secondary IP address subnet pool if the first subnet pool is exhausted or the server ignores further requests. This enhancement is useful if the number of hosts is greater than the number of IP addresses in the pool or if multiple subnets are configured on an interface using secondary addresses.

Related Topics

Enabling or Disabling DHCP Smart Relay Globally, on page 539
Enabling or Disabling DHCP Smart Relay on a Layer 3 Interface, on page 540

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 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. For general information about VRFs, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

Virtualization Support for DHCP

The following information applies to DHCP used in virtual device contexts (VDCs):

- DHCP snooping binding databases are unique per VDC. Bindings in one VDC do not affect DHCP snooping in other VDCs.
- The system does not limit the binding database size on a per-VDC basis.
- The DHCP smart relay agent can be configured independently in default and nondefault VDCs.

Prerequisites for DHCP

DHCP has the following prerequisite:

- You should be familiar with DHCP before you configure DHCP snooping or the DHCP relay agent.

Guidelines and Limitations for DHCP

DHCP has the following configuration guidelines and limitations:

- If you are using both the Unicast reverse Packeting Forwarding (uRFP) strict mode in your client vPC VLANs and the First Hop Redundancy Protocol (FHRP) with the DHCP relay feature, the DHCP requests are sourced from the physical egress IP address interface (not the FHRP VIP) by default. Consequently, if your DHCP server is not on a directly connected subnet and you have multiple ECMP routes back to your vPC pair, some packets might land on the neighbor switch instead of the originating switch and be dropped by RFP. This behavior is expected. To avoid this scenario, perform one of the following workarounds:

- Use the uRFP loose mode, not uRFP strict.
- Configure static routes for the interface address on the affected FHRP interfaces and redistribute the static routes into IGP.

- Using the **ip dhcp relay source-interface** *interface-name*command, you can configure a different interface as the source interface. This command is used for DHCP relay in VPN and in non-VPN environments. The dhcp relay information option with vpn sub-option must be enabled for this command configuration to work. To enable VRF support for the DHCP relay agent, use the **ip dhcp relay information option vpn** command. For more details about the **ip dhcp relay information option vpn** command, see the Cisco Nexus 7000 Series Security Command Reference.
- For Cisco NX-OS Release 6.2 and later releases, you must enable the insertion of Option 82 information for DHCP packets to support the highest DHCP snooping scale.
- After System Switchover, DHCP Global stats show incorrect values as they are not stored in PSS and get erased. Updating stats in PSS during packet path will affect scale.
- If you use DHCP relay where DHCP clients and servers are in different VRF instances, use only one DHCP server within a VRF.
- Before globally enabling DHCP snooping on the device, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
- DHCP snooping does not work with DHCP relay configured on the same nexus device.
- 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. When both DHCP snooping and DHCP relay are enabled on a VLAN and the SVI of that VLAN, DHCP relay takes precedence.
- If an ingress router ACL is configured on a Layer 3 interface that you are configuring with a DHCP server address, ensure that the router ACL permits DHCP traffic between DHCP servers and DHCP hosts.
- Access-control list (ACL) statistics are not supported if the DHCP snooping feature is enabled.
- Make sure that the DHCP configuration is synchronized across the devices in a vPC link. Otherwise, a run-time error can occur, resulting in dropped packets.
- Beginning with Cisco NX-OS Release 5.1, DHCP snooping is supported with FabricPath. Follow these guidelines when enabling DHCP snooping in a FabricPath network:
    - DHCP snooping should be enabled on CE-FabricPath boundary devices.
    - DHCP snooping is enabled on all access layer devices to secure the network at the access layer itself.
    - DHCP does not learn any binding entries on ports in FabricPath mode as users should have enabled DHCP snooping on all access layer devices. As a result, when DAI is enabled, ARP packets received on FabricPath ports are allowed.
    - IPSG cannot be enabled on ports in FabricPath mode.

> **Note** For more information on FabricPath, see the *Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*.

- DHCP smart relay and DHCP subnet broadcast support are limited to the first 100 IP addresses of the interface on which they are enabled.
- You must configure a helper address on the interface in order to use DHCP smart relay and DHCP subnet broadcast support.
- In a vPC environment with DHCP smart relay enabled, the subnet of the primary and secondary addresses of an interface should be the same on both Cisco NX-OS devices.
- Before using POAP, make sure that DHCP snooping is enabled and firewall rules are set to block unintended or malicious DHCP servers.
- When you configure DHCPv6 server addresses on an interface, a destination interface cannot be used with global IPv6 addresses.

> **Note** For DHCP configuration limits, see the *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*.

Default Settings for DHCP

This table lists the default settings for DHCP parameters.

Table 36: Default DHCP Parameters

Parameters	Default
DHCP feature	Disabled
DHCP snooping	Disabled
DHCP snooping on VLANs	Disabled
DHCP snooping MAC address verification	Enabled
DHCP snooping Option 82 support	Disabled
DHCP snooping trust	Untrusted
DHCP relay agent	Enabled
DHCPv6 relay agent	Enabled
Lightweight DHCPv6 Relay Agent	Disabled
UDP Relay feature	Disabled

Parameters	Default
VRF support for the DHCP relay agent	Disabled
VRF support for the DHCPv6 relay agent	Disabled
DHCP relay sub-option type cisco	Disabled
DHCPv6 relay option type cisco	Disabled
DHCP Option 82 for relay agent	Disabled
Subnet broadcast support for the DHCP relay agent	Disabled
DHCP smart relay agent	Disabled
DHCP server IP address	None

Configuring DHCP

Minimum DHCP Configuration

Step 1 Enable the DHCP feature.

When the DHCP feature is disabled, you cannot configure DHCP snooping.

Step 2 Enable DHCP snooping globally.

Step 3 Enable DHCP snooping on at least one VLAN.

By default, DHCP snooping is disabled on all VLANs.

Step 4 Ensure that the DHCP server is connected to the device using a trusted interface.

Step 5 (Optional) If DHCP servers and clients are in different VRF instances, do the following:

a) Enable Option 82 for the DHCP relay agent.
b) Enable VRF support for the DHCP relay agent.

Step 6 (Optional) Configure an interface with the IP address of the DHCP server.

Related Topics

Enabling or Disabling the DHCP Feature, on page 521
Enabling or Disabling DHCP Snooping Globally, on page 521
Enabling or Disabling DHCP Snooping on a VLAN, on page 522
Configuring an Interface as Trusted or Untrusted, on page 526
Enabling or Disabling the DHCP Relay Agent, on page 531
Enabling or Disabling Option 82 for the DHCP Relay Agent, on page 534
Configuring DHCP Server Addresses on an Interface, on page 537
Enabling or Disabling VRF Support for the DHCP Relay Agent, on page 535

Enabling or Disabling the DHCP Feature

You can enable or disable the DHCP feature on the device. By default, DHCP is disabled.

When the DHCP feature is disabled, you cannot configure DHCP snooping, the DHCP relay agent, or any of the features that depend on DHCP, such as dynamic ARP inspection and IP Source Guard. In addition, all DHCP, dynamic ARP inspection, and IP Source Guard configuration is removed from the device.

SUMMARY STEPS

1. **config t**
2. [**no**] **feature dhcp**
3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **feature dhcp** **Example:** `switch(config)# feature dhcp`	Enables the DHCP feature. The **no** option disables the DHCP feature and erases all DHCP configuration.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP 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.

Related Topics

Enabling or Disabling DHCP Snooping Globally, on page 521

Enabling or Disabling DHCP Snooping Globally

You can enable or disable DHCP snooping globally on the device.

Before you begin

Ensure that you have enabled the DHCP feature.

SUMMARY STEPS

1. **config t**
2. [**no**] **ip dhcp snooping**
3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp snooping** **Example:** `switch(config)# ip dhcp snooping`	Enables DHCP snooping globally. The **no** option disables DHCP snooping.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP 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.

Related Topics

Enabling or Disabling the DHCP Feature, on page 521

Enabling or Disabling DHCP Snooping on a VLAN

You can enable or disable DHCP snooping on one or more VLANs. By default, DHCP snooping is disabled on all VLANs.

Before you begin

Ensure that the DHCP feature 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.

SUMMARY STEPS

1. **config t**
2. [**no**] **ip dhcp snooping vlan** *vlan-list*

3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp snooping vlan** *vlan-list* **Example:** `switch(config)# ip dhcp snooping vlan 100,200,250-252`	Enables DHCP snooping on the VLANs specified by *vlan-list*. The **no** option disables DHCP snooping on the VLANs specified.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP 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.

Related Topics

Enabling or Disabling the DHCP Feature, on page 521

Enabling or Disabling DHCP Snooping MAC Address Verification

You can enable or disable DHCP snooping MAC address verification. If the device receives a packet on an untrusted interface and the source MAC address and the DHCP client hardware address do not match, address verification causes the device to drop the packet. MAC address verification is enabled by default.

Before you begin

Ensure that the DHCP feature is enabled.

SUMMARY STEPS

1. **config t**
2. [**no**] **ip dhcp snooping verify mac-address**
3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp snooping verify mac-address** **Example:** `switch(config)# ip dhcp snooping verify mac-address`	Enables DHCP snooping MAC address verification. The **no** option disables MAC address verification.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP 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.

Related Topics

Enabling or Disabling the DHCP Feature, on page 521

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. By default, the device does not include Option 82 information in DHCP packets.

Note DHCP relay agent support for Option 82 is configured separately.

Note To support a higher DHCP pps scale, you must enable the insertion of Option 82 information for DHCP packets.

Before you begin

Ensure that the DHCP feature is enabled.

SUMMARY STEPS

1. **config t**
2. [**no**] **ip dhcp snooping information option**
3. (Optional) **show running-config dhcp**

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

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp snooping information option** **Example:** `switch(config)# ip dhcp snooping information option`	Enables the insertion and removal of Option 82 information for DHCP packets. The **no** option disables the insertion and removal of Option 82 information.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP 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.

Related Topics

Enabling or Disabling the DHCP Feature, on page 521
Enabling or Disabling Option 82 for the DHCP Relay Agent, on page 534

Enabling or Disabling Strict DHCP Packet Validation

You can enable or disable the strict validation of DHCP packets. By default, strict validation of DHCP packets is disabled.

SUMMARY STEPS

1. **config t**
2. [**no**] **ip dhcp packet strict-validation**
3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 2	[**no**] **ip dhcp packet strict-validation** **Example:** `switch(config)# ip dhcp packet strict-validation`	Enables the strict validation of DHCP packets. The **no** option disables strict DHCP packet validation.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP 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 an Interface as Trusted or Untrusted

You can configure whether an interface is a trusted or untrusted source of DHCP messages. By default, all interfaces are untrusted. You can configure DHCP trust on the following types of interfaces:

- Layer 2 Ethernet interfaces
- Layer 2 port-channel interfaces

Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the interface is configured as a Layer 2 interface.

SUMMARY STEPS

1. **config t**
2. Do one of the following options:
   - **interface ethernet** *slot*/*port*
   - **interface port-channel** *channel-number*
3. [**no**] **ip dhcp snooping trust**
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	Do one of the following options:
	• **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*/*port* is the Layer 2 Ethernet interface that you want to configure as trusted or untrusted for DHCP snooping.
		• Enters interface configuration mode, where *slot*/*port* is the Layer 2 port-channel interface that you want to configure as trusted or untrusted for DHCP snooping.

Step 3	[**no**] **ip dhcp snooping trust** **Example:** `switch(config-if)# ip dhcp snooping trust`	Configures the interface as a trusted interface for DHCP snooping. The **no** option configures the port as an untrusted interface.
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config-if)# show running-config dhcp`	Displays the DHCP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling or Disabling the DHCP Feature, on page 521

Enabling or Disabling DHCP Relay Trusted Port Functionality

You can enable or disable the DHCP relay trusted port functionality. By default, if the gateway address is set to all zeros in the DHCP packet and the relay information option is already present in the packet, the DHCP relay agent will not discard the packet. If the **ip dhcp relay information option trust** command is configured globally, the DHCP relay agent will discard the packet if the gateway address is set to all zeros.

Before you begin

Ensure that the DHCP feature is enabled.

SUMMARY STEPS

1. **config t**
2. [**no**] **ip dhcp relay information option trust**
3. (Optional) **show ip dhcp relay**
4. (Optional) **show ip dhcp relay information trusted-sources**
5. (Optional) **show running-config dhcp**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp relay information option trust** **Example:** `switch(config)# ip dhcp relay information option trust`	Enables the DHCP relay trusted port functionality. The **no** option disables this functionality.
Step 3	(Optional) **show ip dhcp relay** **Example:** `switch(config)# show ip dhcp relay`	Displays the DHCP relay configuration.
Step 4	(Optional) **show ip dhcp relay information trusted-sources** **Example:** `switch(config)# show ip dhcp relay information trusted-sources`	Displays the DHCP relay trusted ports configuration.
Step 5	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP 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.

Configuring an Interface as a DHCP Relay Trusted or Untrusted Port

You can configure whether a Layer 3 interface is a DHCP relay trusted or untrusted interface. By default, all interfaces are untrusted. You can configure DHCP relay trust on the following types of interfaces:

- Layer 3 Ethernet interfaces and sub-interfaces
- Layer 3 port-channel interfaces
- Interface VLAN

Before you begin

Ensure that the DHCP feature is enabled.

SUMMARY STEPS

1. **config t**

2. Do one of the following options:
   - **interface ethernet** *slot*/*port*.[*number*]
   - **interface port-channel** *channel-number*.[*subchannel-id*]
   - **interface vlan** *vlan-id*
3. [**no**] **ip dhcp relay information trusted**
4. **show ip dhcp relay information trusted-sources**
5. (Optional) **show running-config dhcp**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	Do one of the following options:
	• **interface ethernet** *slot*/*port*.[*number*]
	• **interface port-channel** *channel-number*.[*subchannel-id*]
	• **interface vlan** *vlan-id*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		• Enters interface configuration mode, where *slot*/*port* is the Layer 3 Ethernet interface that you want to configure as trusted or untrusted.
		• Enters interface configuration mode, where *channel-number* is the Layer 3 port-channel interface that you want to configure as trusted or untrusted.
		• Enters interface configuration mode, where *vlan-id* is the VLAN interface that you want to configure as trusted or untrusted.

Step 3	[**no**] **ip dhcp relay information trusted** **Example:** `switch(config-if)# ip dhcp relay information trusted`	Configures the interface as a trusted interface for DHCP relay agent information. The **no** option configures the port as an untrusted interface. **Note** For any L3 interface, if the interface is configured as trusted either through global command or interface-level command, the interface is considered as a trusted interface. Hence, when the trusted-port command is enabled at Global level, any L3 interface cannot be considered as untrusted irrespective of the interface-level configuration.
Step 4	**show ip dhcp relay information trusted-sources** **Example:** `switch(config-if)# show ip dhcp relay information trusted-sources`	Displays the DHCP relay trusted ports configuration.
Step 5	(Optional) **show running-config dhcp** **Example:**	Displays the DHCP configuration.

	Command or Action	Purpose
	`switch(config-if)# show running-config dhcp`	
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring all Interfaces as Trusted or Untrusted

You can configure all Layer 3 interfaces as DHCP relay trusted or untrusted interfaces. By default, all interfaces are untrusted. You can configure DHCP relay trust on the following types of interfaces:

- Layer 3 Ethernet interfaces and sub-interfaces
- Layer 3 port-channel interfaces
- Interface VLAN

When you enable the **ip dhcp relay information trust-all** command, any Layer 3 interface cannot be considered as untrusted irrespective of the interface-level configuration.

Before you begin

Ensure that the DHCP feature is enabled.

SUMMARY STEPS

1. **config t**
2. [**no**] **ip dhcp relay information trust-all**
3. **show ip dhcp relay information trusted-sources**
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp relay information trust-all** **Example:** `switch(config)# ip dhcp relay information trust-all`	Configures the interfaces as trusted sources of DHCP messages. The **no** option configures the ports as untrusted interfaces.
Step 3	**show ip dhcp relay information trusted-sources** **Example:**	Displays the DHCP relay trusted ports configuration.

	Command or Action	Purpose
	`switch(config)# show ip dhcp relay information trusted-sources`	
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

SUMMARY STEPS

1. **config t**
2. [**no**] **ip dhcp relay**
3. (Optional) **show ip dhcp relay**
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp relay** **Example:** `switch(config)# ip dhcp relay`	Enables the DHCP relay agent. The **no** option disables the relay agent.
Step 3	(Optional) **show ip dhcp relay** **Example:** `switch(config)# show ip dhcp relay`	Displays the DHCP relay configuration.
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.

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

Related Topics

Enabling or Disabling the DHCP Feature, on page 521

Enabling or Disabling the DHCP Relay Source Interface

You can enable or disable the DHCP relay source interface. You can configure a different interface as the source of the DHCP relay agent.

Before you begin

Ensure that the DHCP feature is enabled.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ip dhcp relay source-interface** *interface-name*
3. [**no**] **ip dhcp relay information option vpn**
4. **interface** *interface-name*
5. [**no**] **ip dhcp relay address** *ip address* **use-vrf** *vrf-name*
6. (Optional) **show ip dhcp relay source-interface**
7. (Optional) **show running-config dhcp**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp relay source-interface** *interface-name* **Example:** `switch(config)# ip dhcp relay source-interface Ethernet1/1`	Enables the DHCP relay source interface. You can configure a different interface as the source of the DHCP relay agent. The **no** option disables the relay source interface. The source interface's IP address will be used as the source address in the DHCP packet, only when the source interface and the DHCP server are in the same VRF. If not in same VRF, IP address of any other interface (through which server will be reachable) will be used.

	Command or Action	Purpose
Step 3	[**no**] **ip dhcp relay information option vpn** **Example:** `switch(config)# ip dhcp relay information option vpn`	Enables VRF support for the DHCP relay agent. The no option disables the VRF support. The VPN option will be added in option-82 only when the server and the client are in the different VRF. Three sub-options get added in the information option of the relayed packet only when the server and client are in different VRFs. Sub-option 151 - VRF Name / VPN ID: this indicates the VRF information of the client. Sub-option 11 - Server ID override: this indicates the client subnet gateway. Sub-option 5 - Link Selection: provides the client subnet address. When the client and server are in different VRFs, the DHCP server address configuration must have **use-vrf** *vrf-name* for the DHCP relay to work.
Step 4	**interface** *interface-name* **Example:** `switch(config)# interface ethernet 1/3`	Configures the interface and enters interface configuration mode.
Step 5	[**no**] **ip dhcp relay address** *ip address* **use-vrf** *vrf-name* **Example:** `switch(config-if)# ip dhcp relay address 10.43.87.132 use-vrf testA`	Configures an IP address for a DHCP server to which the relay agent forwards the packets received on this interface. The **use-vrf** option specifies the virtual routing and forwarding instance (VRF) that the DHCP server is within, where the vrf-name argument is the name of the VRF. The VRF membership of the interface connected to the DHCP server determines the VRF that the DHCP is within. The source interface's IP address will be used as the source address only when the source interface and the server are in the same VRF.
Step 6	(Optional) **show ip dhcp relay source-interface** **Example:** `switch(config)# show ip dhcp relay source-interface`	Displays the DHCP relay source-interface configuration.
Step 7	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ip dhcp relay**
3. [**no**] **ip dhcp relay information option**
4. (Optional) **show ip dhcp relay**
5. (Optional) **show running-config dhcp**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp relay** **Example:** `switch(config)# ip dhcp relay`	Enables the DHCP relay feature. The **no** option disables this behavior.
Step 3	[**no**] **ip dhcp relay information option** **Example:** `switch(config)# ip dhcp relay information option`	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 **no** option disables this behavior.
Step 4	(Optional) **show ip dhcp relay** **Example:** `switch(config)# show ip dhcp relay`	Displays the DHCP relay configuration.
Step 5	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

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.

SUMMARY STEPS

1. **config t**
2. [**no**] **ip dhcp relay information option vpn**
3. [**no**] **ip dhcp relay sub-option type cisco**
4. (Optional) **show ip dhcp relay**
5. (Optional) **show running-config dhcp**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp relay information option vpn** **Example:** `switch(config)# ip dhcp relay information option vpn`	Enables VRF support for the DHCP relay agent. The **no** option disables this behavior.
Step 3	[**no**] **ip dhcp relay sub-option type cisco** **Example:** `switch(config)# ip dhcp relay sub-option type cisco`	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent Option 82 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.
Step 4	(Optional) **show ip dhcp relay** **Example:** `switch(config)# show ip dhcp relay`	Displays the DHCP relay configuration.
Step 5	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

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

Related Topics

Enabling or Disabling Option 82 for the DHCP Relay Agent, on page 534
VRF Support for the DHCP Relay Agent, on page 516

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.

SUMMARY STEPS

1. **config t**
2. **interface** *interface slot/port*
3. [**no**] **ip dhcp relay subnet-broadcast**
4. **exit**
5. **exit**
6. (Optional) **show ip dhcp relay**
7. (Optional) **show running-config dhcp**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *interface slot/port*
	Example:
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		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.

Step 3	[**no**] **ip dhcp relay subnet-broadcast** **Example:** `switch(config-if)# ip dhcp relay subnet-broadcast`	Enables subnet broadcast support for the DHCP relay agent. The **no** option disables this behavior.

	Command or Action	Purpose

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 6	(Optional) **show ip dhcp relay** **Example:** `switch# show ip dhcp relay`	Displays the DHCP relay configuration.
Step 7	(Optional) **show running-config dhcp** **Example:** `switch# show running-config dhcp`	Displays the DHCP configuration.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring DHCP Server Addresses on an Interface

You can configure DHCP server IP addresses on an interface. When an inbound DHCP BOOTREQUEST packet arrives on the interface, the relay agent forwards the packet to all DHCP server IP addresses specified. The relay agent forwards replies from all DHCP servers to the host that sent the request.

Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the DHCP server is correctly configured.

Determine the IP address for each DHCP server that you want to configure on the interface.

If the DHCP server is in a different VRF instance than the interface, ensure that you have enabled VRF support.

Note If an ingress router ACL is configured on an interface that you are configuring with a DHCP server address, ensure that the router ACL permits DHCP traffic between DHCP servers and DHCP hosts.

SUMMARY STEPS

1. **config t**
2. Do one of the following options:

- **interface ethernet** *slot*/*port*[**.** *number*]
- **interface vlan** *vlan-id*
- **interface port-channel** *channel-id*[.*subchannel-id*]

3. **ip dhcp relay address** *IP-address* [**use-vrf** *vrf-name*]
4. (Optional) **show ip dhcp relay address**
5. (Optional) **show running-config dhcp**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	Do one of the following options:
	• **interface ethernet** *slot*/*port*[**.** *number*]
	• **interface vlan** *vlan-id*
	• **interface port-channel** *channel-id*[.*subchannel-id*]
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		• Enters interface configuration mode, where *slot*/*port* is the physical Ethernet interface that you want to configure with a DHCP server IP address. If you want to configure a subinterface, include the *number* argument to specify the subinterface number.
		• Enters interface configuration mode, where *vlan-id* is the ID of the VLAN that you want to configure with a DHCP server IP address.
		• Enters interface configuration mode, where *channel-id* is the ID of the port channel that you want to configure with a DHCP server IP address. If you want to configure a subchannel, include the *subchannel-id* argument to specify the subchannel ID.

Step 3	**ip dhcp relay address** *IP-address* [**use-vrf** *vrf-name*] **Example:** `switch(config-if)# ip dhcp relay address 10.132.7.120 use-vrf red`	Configures an IP address for a DHCP server to which the relay agent forwards BOOTREQUEST packets received on this interface. To configure more than one IP address, use the **ip dhcp relay address** command once per address.
Step 4	(Optional) **show ip dhcp relay address** **Example:** `switch(config-if)# show ip dhcp relay address`	Displays all the configured DHCP server addresses.
Step 5	(Optional) **show running-config dhcp** **Example:** `switch(config-if)# show running-config dhcp`	Displays the DHCP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	`switch(config-if)# copy running-config startup-config`	

Related Topics

Enabling or Disabling the DHCP Feature, on page 521

Enabling or Disabling DHCP Smart Relay Globally

You can enable or disable DHCP smart relay globally on the device.

Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the DHCP relay agent is enabled.

SUMMARY STEPS

1. **config t**
2. [**no**] **ip dhcp smart-relay global**
3. (Optional) **show ip dhcp relay**
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip dhcp smart-relay global** **Example:** `switch(config)# ip dhcp smart-relay global`	Enables DHCP smart relay globally. The **no** option disables DHCP smart relay.
Step 3	(Optional) **show ip dhcp relay** **Example:** `switch(config)# show ip dhcp relay`	Displays the DHCP smart relay configuration.
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling or Disabling DHCP Smart Relay on a Layer 3 Interface

You can enable or disable DHCP smart relay on Layer 3 interfaces.

Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the DHCP relay agent is enabled.

SUMMARY STEPS

1. **config t**
2. **interface** *interface slot*/*port*
3. [**no**] **ip dhcp smart-relay**
4. **exit**
5. **exit**
6. (Optional) **show ip dhcp relay**
7. (Optional) **show running-config dhcp**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *interface slot*/*port*
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		Enters interface configuration mode, where *slot*/*port* is the interface for which you want to enable or disable DHCP smart relay.

Step 3	[**no**] **ip dhcp smart-relay** **Example:** `switch(config-if)# ip dhcp smart-relay`	Enables DHCP smart relay on the interface. The **no** option disables DHCP smart relay on the interface.

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

	Command or Action	Purpose
Step 6	(Optional) **show ip dhcp relay** **Example:** `switch# show ip dhcp relay`	Displays the DHCP smart relay configuration.
Step 7	(Optional) **show running-config dhcp** **Example:** `switch# show running-config dhcp`	Displays the DHCP configuration.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring DHCPv6

Enabling or Disabling the DHCPv6 Relay Agent

You can enable or disable the DHCPv6 relay agent. By default, the DHCPv6 relay agent is enabled.

Before you begin

Ensure that the DHCP feature is enabled.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ipv6 dhcp relay**
3. (Optional) **show ipv6 dhcp relay** [**interface** *interface*]
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure 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.

	Command or Action	Purpose
Step 3	(Optional) **show ipv6 dhcp relay** [**interface** *interface*] **Example:** `switch(config)# show ipv6 dhcp relay`	Displays the DHCPv6 relay configuration.
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup 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.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ipv6 dhcp relay option vpn**
3. [**no**] **ipv6 dhcp relay option type cisco**
4. (Optional) **show ipv6 dhcp relay** [**interface** *interface*]
5. (Optional) **show running-config dhcp**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ipv6 dhcp relay option vpn** **Example:** `switch(config)# ipv6 dhcp relay option vpn`	Enables VRF support for the DHCPv6 relay agent. The **no** option disables this behavior.

	Command or Action	Purpose
Step 3	[**no**] **ipv6 dhcp relay option type cisco** **Example:** `switch(config)# ipv6 dhcp relay option type cisco`	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.
Step 4	(Optional) **show ipv6 dhcp relay** [**interface** *interface*] **Example:** `switch(config)# show ipv6 dhcp relay`	Displays the DHCPv6 relay configuration.
Step 5	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP 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.

Configuring DHCPv6 Server Addresses on an Interface

You can configure DHCPv6 server IP addresses on an interface. When an inbound DHCP BOOTREQUEST packet arrives on the interface, the relay agent forwards the packet to all DHCPv6 server IP addresses specified. The relay agent forwards replies from all DHCPv6 servers to the host that sent the request.

Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the DHCPv6 server is correctly configured.

Determine the IP address for each DHCPv6 server that you want to configure on the interface.

If the DHCPv6 server is in a different VRF than the interface, ensure that you have enabled VRF support.

Note If an ingress router ACL is configured on an interface that you are configuring with a DHCPv6 server address, ensure that the router ACL permits DHCP traffic between DHCPv6 servers and DHCP hosts.

SUMMARY STEPS

1. **config t**
2. Do one of the following options:
   - **interface ethernet** *slot*/*port*[**.** *number*]
   - **interface port-channel** *channel-id*[.*subchannel-id*]

3. [**no**] **ipv6 dhcp relay address** *IPv6-address* [**use-vrf** *vrf-name*] [**interface** *interface*]
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	Do one of the following options:
	• **interface ethernet** *slot*/*port*[**.** *number*]
	• **interface port-channel** *channel-id*[.*subchannel-id*]
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		• Enters interface configuration mode, where *slot*/*port* is the physical Ethernet interface that you want to configure with a DHCPv6 server IP address. If you want to configure a subinterface, include the *number* argument to specify the subinterface number.
		• Enters interface configuration mode, where *channel-id* is the ID of the port channel that you want to configure with a DHCPv6 server IP address. If you want to configure a subchannel, include the *subchannel-id* argument to specify the subchannel ID.

Step 3	[**no**] **ipv6 dhcp relay address** *IPv6-address* [**use-vrf** *vrf-name*] [**interface** *interface*] **Example:** `switch(config-if)# ipv6 dhcp relay address FF02:1::FF0E:8C6C use-vrf red`	Configures an IP address for a DHCPv6 server to which the relay agent forwards BOOTREQUEST packets received on this interface. Use the **use-vrf** option to specify the VRF name of the server if it is in a different VRF and the other argument interface is used to specify the output interface for the destination. The server address can either be a link-scoped unicast or multicast address or a global or site-local unicast or multicast address. The **interface** option is mandatory for a link-scoped server address and multicast address. It is not allowed for a global or site-scoped server address. To configure more than one IP address, use the **ipv6 dhcp relay address** command once per address.
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config-if)# show running-config dhcp`	Displays the DHCPv6 configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring the 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.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ipv6 dhcp relay source-interface** *interface*
3. (Optional) **show ipv6 dhcp relay** [**interface** *interface*]
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ipv6 dhcp relay source-interface** *interface* **Example:** `switch(config)# ipv6 dhcp relay source-interface loopback 2`	Configures the source interface for the DHCPv6 relay agent. **Note** 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.
Step 3	(Optional) **show ipv6 dhcp relay** [**interface** *interface*] **Example:** `switch(config)# show ipv6 dhcp relay`	Displays the DHCPv6 relay configuration.
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the DHCP Configuration

To display DHCP configuration information, perform one of the following tasks. For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
show running-config dhcp [**all**]	Displays the DHCP configuration in the running configuration.
show ip dhcp relay	Displays the DHCP relay configuration.
show ipv6 dhcp relay [**interface** *interface*]	Displays the DHCPv6 relay global or interface-level configuration.
show ip dhcp relay address	Displays all the DHCP server addresses configured on the device.
show ip dhcp snooping	Displays general information about DHCP snooping.
show startup-config dhcp [**all**]	Displays the DHCP configuration in the startup configuration.

Displaying DHCP Bindings

Use the **show ip dhcp snooping binding** command to display the DHCP binding table. For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

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 the DHCP feature is enabled.

SUMMARY STEPS

1. (Optional) **clear ip dhcp snooping binding**
2. (Optional) **clear ip dhcp snooping binding interface ethernet** *slot*/*port*[.*subinterface-number*]
3. (Optional) **clear ip dhcp snooping binding interface port-channel** *channel-number*[.*subchannel-number*]
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*] }

5. (Optional) **show ip dhcp snooping binding**

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **clear ip dhcp snooping binding** **Example:** `switch# clear ip dhcp snooping binding`	Clears all entries from the DHCP snooping binding database.
Step 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.
Step 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.
Step 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.
Step 5	(Optional) **show ip dhcp snooping binding** **Example:** `switch# show ip dhcp snooping binding`	Displays the DHCP snooping binding database.

Related Topics

Enabling or Disabling the DHCP Feature, on page 521

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.

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.

Monitoring DHCP

Use the **show ip dhcp snooping statistics** command to monitor DHCP snooping.

Use the **show ip dhcp relay statistics** [**interface** *interface*] command to monitor DHCP relay statistics at the global 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.

Use the **show ipv6 dhcp relay statistics** [**interface** *interface*] command to monitor DHCPv6 relay statistics at the global or interface level.

Note For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Additional References for DHCP

Related Documents

Related Topic	Document Title
DHCP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
VRFs and Layer 3 virtualization	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*
vPCs	*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*

Standards

Standards	Title
RFC-2131	Dynamic Host Configuration Protocol
RFC-3046	DHCP Relay Agent Information Option

Standards	Title
RFC-6607	Virtual Subnet Selection Options for DHCPv4 and DHCPv6

Feature History for DHCP

This table lists the release history for this feature.

Table 37: Feature History for DHCP

Feature Name	Releases	Feature Information
IP DHCP Relay Source Interface	8.2(3)	Added support for the DHCP relay source interface.
DHCP	6.2(2)	Added support for the DHCPv6 relay agent.
DHCP	6.2(2)	Added a new default circuit ID format that is used when Option 82 is enabled for DHCP snooping.
DHCP	6.0(1)	No change from Release 5.2.
DHCP	5.2(1)	Added support for DHCP smart relay.
DHCP	5.2(1)	Added subnet broadcast support for the DHCP relay agent.
DHCP	5.1(1)	Optimized DHCP snooping to work in a vPC environment.
DHCP	5.0(2)	Modified the DHCP relay agent to support VRFs, added the **ip dhcp relay information option vpn** command, and modified the **ip dhcp relay address** command to add the **use-vrf** *vrf-name* option.

Feature Name	Releases	Feature Information
DHCP	5.0(2)	Added the **ip dhcp relay sub-option type cisco** command to enable DHCP to use Cisco proprietary numbers 150, 152, and 151 for the link selection, server ID override, and VRF name/VPN ID relay agent Option 82 suboptions.
DHCP	4.2(1)	Deprecated the **service dhcp** command and replaced it with the **ip dhcp relay** command.

CHAPTER 19

Configuring Dynamic ARP Inspection

This chapter describes how to configure dynamic Address Resolution Protocol (ARP) inspection (DAI) on a Cisco NX-OS device.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About DAI

ARP

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, host B wants to send information to host A but does not have the MAC address of host A in its ARP cache. In ARP terms, host B is the sender and host A is the target.

To get the MAC address of host A, host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of host A. All hosts within the broadcast domain receive the ARP request, and host A responds with its MAC address.

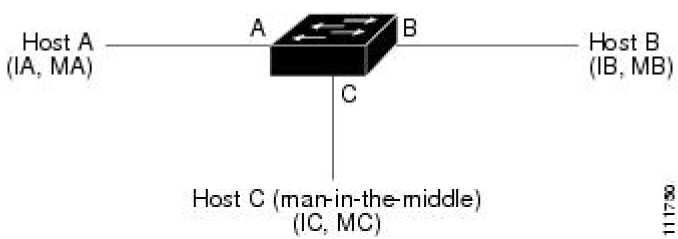
ARP Spoofing Attacks

ARP spoofing attacks and ARP cache poisoning can occur because ARP allows a reply from a host even if an ARP request was not received. After the attack, all traffic from the device under attack flows through the attacker's computer and then to the router, switch, or host.

An ARP spoofing attack can affect hosts, switches, and routers connected to your Layer 2 network by sending false information to the ARP caches of the devices connected to the subnet. Sending false information to an ARP cache is known as ARP cache poisoning. Spoof attacks can also intercept traffic intended for other hosts on the subnet.

Figure 24: ARP Cache Poisoning

This figure shows an example of ARP cache poisoning.



Hosts A, B, and C are connected to the device on interfaces A, B, and C, which are on the same subnet. Their IP and MAC addresses are shown in parentheses; for example, host A uses IP address IA and MAC address MA. When host A needs to send IP data to host B, it broadcasts an ARP request for the MAC address associated with IP address IB. When the device and host B receive the ARP request, they populate their ARP caches with an ARP binding for a host with the IP address IA and a MAC address MA; for example, IP address IA is bound to MAC address MA. When host B responds, the device and host A populate their ARP caches with a binding for a host with the IP address IB and the MAC address MB.

Host C can poison the ARP caches of the device, host A, and host B by broadcasting two forged ARP responses with bindings: one for a host with an IP address of IA and a MAC address of MC and another for a host with the IP address of IB and a MAC address of MC. Host B and the device then use the MAC address MC as the destination MAC address for traffic intended for IA, which means that host C intercepts that traffic. Likewise, host A and the device use the MAC address MC as the destination MAC address for traffic intended for IB.

Because host C knows the true MAC addresses associated with IA and IB, it can forward the intercepted traffic to those hosts by using the correct MAC address as the destination. This topology, in which host C has inserted itself into the traffic stream from host A to host B, is an example of a *man-in-the middle* attack.

DAI and ARP Spoofing Attacks

DAI ensures that only valid ARP requests and responses are relayed. When DAI is enabled and properly configured, a Cisco Nexus device performs these activities:

- Intercepts all ARP requests and responses on untrusted ports
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination
- Drops invalid ARP packets

DAI can determine the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a Dynamic Host Configuration Protocol (DHCP) snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the device. It can also contain static entries that you create. If the ARP packet is received on a trusted interface, the device forwards the packet without any checks. On untrusted interfaces, the device forwards the packet only if it is valid.

DAI can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses. The device logs dropped packets.

You can configure DAI to drop ARP packets when the IP addresses in the packets are invalid or when the MAC addresses in the body of the ARP packets do not match the addresses specified in the Ethernet header.

Related Topics

Applying ARP ACLs to VLANs for DAI Filtering, on page 559
Logging DAI Packets, on page 555
Enabling or Disabling Additional Validation, on page 560

Interface Trust States and Network Security

DAI associates a trust state with each interface on the device. Packets that arrive on trusted interfaces bypass all DAI validation checks, and packets that arrive on untrusted interfaces go through the DAI validation process.

In a typical network configuration, the guidelines for configuring the trust state of interfaces are as follows:

Untrusted

Interfaces that are connected to hosts

Trusted

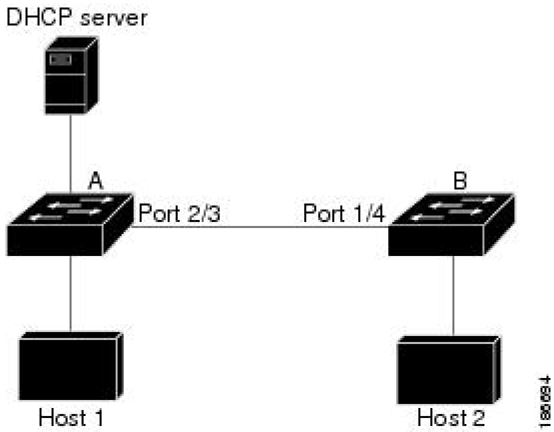
Interfaces that are connected to devices

With this configuration, all ARP packets that enter the network from a device bypass the security check. No other validation is needed at any other place in the VLAN or in the network.

Caution Use the trust state configuration carefully. Configuring interfaces as untrusted when they should be trusted can result in a loss of connectivity.

Figure 25: ARP Packet Validation on a VLAN Enabled for DAI

The following figure, assume that both device A and device B are running DAI on the VLAN that includes host 1 and host 2. If host 1 and host 2 acquire their IP addresses from the DHCP server connected to device A, only device A binds the IP-to-MAC address of host 1. If the interface between device A and device B is untrusted, the ARP packets from host 1 are dropped by device B and connectivity between host 1 and host 2 is lost.



If you configure interfaces as trusted when they should be untrusted, you may open a security hole in a network. If device A is not running DAI, host 1 can easily poison the ARP cache of device B (and host 2, if you configured the link between the devices as trusted). This condition can occur even though device B is running DAI.

DAI ensures that hosts (on untrusted interfaces) connected to a device that runs DAI do not poison the ARP caches of other hosts in the network; however, DAI does not prevent hosts in other portions of the network from poisoning the caches of the hosts that are connected to a device that runs DAI.

If some devices in a VLAN run DAI and other devices do not, the guidelines for configuring the trust state of interfaces on a device that runs DAI becomes the following:

Untrusted

Interfaces that are connected to hosts or to devices that *are not* running DAI

Trusted

Interfaces that are connected to devices that *are* running DAI

To validate the bindings of packets from devices that do not run DAI, configure ARP ACLs on the device that runs DAI. When you cannot determine the bindings, isolate at Layer 3 the devices that run DAI from devices that do not run DAI.

Note Depending on your network setup, you may not be able to validate a given ARP packet on all devices in the VLAN.

Related Topics

Configuring the DAI Trust State of a Layer 2 Interface, on page 558
Example 2 One Device Supports DAI, on page 568

Prioritizing ARP ACLs and DHCP Snooping Entries

By default, DAI filters DAI traffic by comparing DAI packets to IP-MAC address bindings in the DHCP snooping database.

When you apply an ARP ACL to traffic, the ARP ACLs take precedence over the default filtering behavior. The device first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the device denies the packet regardless of whether a valid IP-MAC binding exists in the DHCP snooping database.

Note VLAN ACLs (VACLs) take precedence over both ARP ACLs and DHCP snooping entries. For example, if you apply a VACL and an ARP ACL to a VLAN and you configured the VACL to act on ARP traffic, the device permits or denies ARP traffic as determined by the VACL, not the ARP ACL or DHCP snooping entries.

Related Topics

Configuring ARP ACLs, on page 570
Applying ARP ACLs to VLANs for DAI Filtering, on page 559

Logging DAI Packets

Cisco NX-OS maintains a buffer of log entries about DAI packets processed. Each log entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.

You can also specify the type of packets that are logged. By default, aCisco Nexus device logs only packets that DAI drops.

If the log buffer overflows, the device overwrites the oldest DAI log entries with newer entries. You can configure the maximum number of entries in the buffer.

Note Cisco NX-OS does not generate system messages about DAI packets that are logged.

Related Topics

Configuring the DAI Logging Buffer Size, on page 561
Configuring DAI Log Filtering, on page 562

Virtualization Support for DAI

The following information applies to DAI used in virtual device contexts (VDCs):

- IP-MAC address bindings are unique per VDC.
- ARP ACLs are unique per VDC. You cannot use an ACL that you created in one VDC in a different VDC.
- Because ACLs are not shared by VDCs, you can reuse ACL names in different VDCs.

- The system does not limit ARP ACLs or rules on a per-VDC basis.

Prerequisites for DAI

- You must enable the DHCP feature before you can configure DAI.

Guidelines and Limitations for DAI

DAI has the following configuration guidelines and limitations:

- DAI is an ingress security feature; it does not perform any egress checking.
- DAI is not effective for hosts connected to devices that do not support DAI or that do not have this feature enabled. Because man-in-the-middle attacks are limited to a single Layer 2 broadcast domain, you should separate the domain with DAI from domains without DAI. This separation secures the ARP caches of hosts in the domain with DAI.
- DAI depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. If you want DAI to use static IP-MAC address bindings to determine if ARP packets are valid, DHCP snooping needs only to be enabled. If you want DAI to use dynamic IP-MAC address bindings to determine if ARP packets are valid, you must configure DHCP snooping on the same VLANs on which you configure DAI.
- When you use the **feature dhcp** command to enable the DHCP feature, there is a delay of approximately 30 seconds before the I/O modules receive the DHCP or DAI configuration. This delay occurs regardless of the method that you use to change from a configuration with the DHCP feature disabled to a configuration with the DHCP feature enabled. For example, if you use the Rollback feature to revert to a configuration that enables the DHCP feature, the I/O modules receive the DHCP and DAI configuration approximately 30 seconds after you complete the rollback.
- When DHCP snooping is disabled or used in a non-DHCP environment, you should use ARP ACLs to permit or to deny packets and disable DAI.
- DAI is supported on access ports, trunk ports, port-channel ports, and private VLAN ports.
- The DAI trust configuration of a port channel determines the trust state of all physical ports that you assign to the port channel. For example, if you have configured a physical port as a trusted interface and then you add that physical port to a port channel that is an untrusted interface, the physical port becomes untrusted.
- When you remove a physical port from a port channel, the physical port does not retain the DAI trust state configuration of the port channel.
- When you change the trust state on the port channel, the device configures a new trust state on all the physical ports that comprise the channel.
- If you want DAI to use static IP-MAC address bindings to determine if ARP packets are valid, ensure that DHCP snooping is enabled and that you have configured the static IP-MAC address bindings.
- If you want DAI to use dynamic IP-MAC address bindings to determine if ARP packets are valid, ensure that DHCP snooping is enabled.

Default Settings for DAI

This table lists the default settings for DAI parameters.

Table 38: Default DAI Parameters

Parameters	Default
DAI	Disabled on all VLANs.
Interface trust state	All interfaces are untrusted.
ARP ACLs for non-DHCP environments	No ARP ACLs are defined.
Validation checks	No checks are performed.
Log buffer	When DAI is enabled, all denied or dropped ARP packets are logged. The number of entries in the log is 32. The number of system messages is limited to 5 per second. The logging-rate interval is 1 second.
Per-VLAN logging	All denied or dropped ARP packets are logged.

Configuring DAI

Enabling or Disabling DAI on VLANs

You can enable or disable DAI on VLANs. By default, DAI is disabled on all VLANs.

Before you begin

If you are enabling DAI, ensure the following:

- Ensure that the DHCP feature is enabled.
- The VLANs on which you want to enable DAI are configured.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ip arp inspection vlan** *list*
3. (Optional) **show ip arp inspection vlan** *list*
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip arp inspection vlan** *list* **Example:** `switch(config)# ip arp inspection vlan 13`	Enables DAI for the specified list of VLANs. The **no** option disables DAI for the specified VLANs.
Step 3	(Optional) **show ip arp inspection vlan** *list* **Example:** `switch(config)# show ip arp inspection vlan 13`	Shows the DAI status for the specified list of VLANs.
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 the DAI Trust State of a Layer 2 Interface

You can configure the DAI interface trust state of a Layer 2 interface. By default, all interfaces are untrusted.

A device forwards ARP packets that it receives on a trusted Layer 2 interface but does not check them.

On untrusted interfaces, the device intercepts all ARP requests and responses and verifies that the intercepted packets have valid IP-MAC address bindings before updating the local cache and forwarding the packet to the appropriate destination. If the device determines that packets have invalid bindings, it drops the packets and logs them according to the logging configuration.

Before you begin

If you are enabling DAI, ensure that the DHCP feature is enabled.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type number* / *slot*
3. [**no**] **ip arp inspection trust**
4. (Optional) **show ip arp inspection interface** *type number* / *slot*
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**interface** *type number* / *slot*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	[**no**] **ip arp inspection trust** **Example:** `switch(config-if)# ip arp inspection trust`	Configures the interface as a trusted ARP interface. The **no** option configures the interface as an untrusted ARP interface.
Step 4	(Optional) **show ip arp inspection interface** *type number* / *slot* **Example:** `switch(config-if)# show ip arp inspection interface ethernet 2/1`	Displays the trust state and the ARP packet rate for the specified interface.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Interface Trust States and Network Security, on page 553
Configuring DAI Log Filtering, on page 562

Applying ARP ACLs to VLANs for DAI Filtering

You can apply an ARP ACL to one or more VLANs. The device permits packets only if the ACL permits them. By default, no VLANs have an ARP ACL applied.

Before you begin

Ensure that the ARP ACL that you want to apply is correctly configured.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ip arp inspection filter** *acl-name* **vlan** *list*
3. (Optional) **show ip arp inspection vlan** *list*
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip arp inspection filter** *acl-name* **vlan** *list* **Example:** `switch(config)# ip arp inspection filter arp-acl-01 vlan 100`	Applies the ARP ACL to the list of VLANs, or if you use the **no** option, removes the ARP ACL from the list of VLANs.
Step 3	(Optional) **show ip arp inspection vlan** *list* **Example:** `switch(config)# show ip arp inspection vlan 100`	Shows the DAI status for the specified list of VLANs, including whether an ARP ACL is applied.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring ARP ACLs, on page 570

Enabling or Disabling Additional Validation

You can enable or disable additional validation of ARP packets. By default, no additional validation of ARP packets is enabled. When no additional validation is configured, the source MAC address and the source IP address check against the IP-to-MAC binding entry for ARP packets are done by using the Ethernet source MAC address (not the ARP sender MAC address) and the ARP sender IP address.

DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. You can enable additional validation on the destination MAC address, the sender and target IP addresses, and the source MAC address.

You can use the following keywords with the **ip arp inspection validate** command to implement additional validations:

dst-mac

Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

ip

Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

src-mac

Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body for ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

When enabling additional validation, follow these guidelines:

- You must specify at least one of the keywords. You can specify one, two, or all three keywords.
- Each **ip arp inspection validate** command that you enter replaces the configuration from any previous commands. If you enter an **ip arp inspection validate** command to enable src-mac and dst-mac validations, and a second **ip arp inspection validate** command to enable ip validation, the src-mac and dst-mac validations are disabled when you enter the second command.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]}
3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} **Example:** `switch(config)# ip arp inspection validate src-mac dst-mac ip`	Enables additional DAI validation, or if you use the **no** option, disables additional DAI validation.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP snooping configuration, including the DAI 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 the DAI Logging Buffer Size

You can configure the DAI logging buffer size. The default buffer size is 32 messages.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ip arp inspection log-buffer entries** *number*
3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip arp inspection log-buffer entries** *number* **Example:** `switch(config)# ip arp inspection log-buffer entries 64`	Configures the DAI logging buffer size. The **no** option reverts to the default buffer size, which is 32 messages. The buffer size can be between 1 and 1024 messages.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP snooping configuration, including the DAI 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 DAI Log Filtering

You can configure how the device determines whether to log a DAI packet. By default, the device logs DAI packets that are dropped.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
   - **ip arp inspection vlan** *vlan-list* **logging dhcp-bindings all**
   - **ip arp inspection vlan** *vlan-list* **logging dhcp-bindings none**
   - **ip arp inspection vlan** *vlan-list* **logging dhcp-bindingspermit**
   - **no ip arp inspection vlan** *vlan-list* **logging dhcp-bindings** {**all** | **none** | **permit**}
3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	Enter one of the following commands: • **ip arp inspection vlan** *vlan-list* **logging dhcp-bindings all** • **ip arp inspection vlan** *vlan-list* **logging dhcp-bindings none** • **ip arp inspection vlan** *vlan-list* **logging dhcp-bindingspermit** • **no ip arp inspection vlan** *vlan-list* **logging dhcp-bindings** {**all** | **none** | **permit**} **Example:** `switch(config)# ip arp inspection vlan 100 dhcp-bindings permit`	Configures DAI log filtering, as follows. The **no** option removes DAI log filtering. • Logs all packets that match DHCP bindings. • Does not log packets that match DHCP bindings. • Logs packets permitted by DHCP bindings. • Removes DAI log filtering.
Step 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	Displays the DHCP snooping configuration, including the DAI 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.

Verifying the DAI Configuration

To display the DAI configuration information, perform one of the following tasks. For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
show ip arp inspection	Displays the status of DAI.
show ip arp inspection interface ethernet	Displays the trust state.
show ip arp inspection vlan	Displays the DAI configuration for a specific VLAN.
show arp access-lists	Displays ARP ACLs.
show ip arp inspection log	Displays the DAI log configuration.

Monitoring and Clearing DAI Statistics

To monitor and clear DAI statistics, use the commands in this table. For more information about these commands, see the *Security Command Reference* for your Cisco Nexus device.

Command	Purpose
show ip arp inspection statistics	Displays DAI statistics.
clear ip arp inspection statistics vlan <id>	Clears DAI statistics.

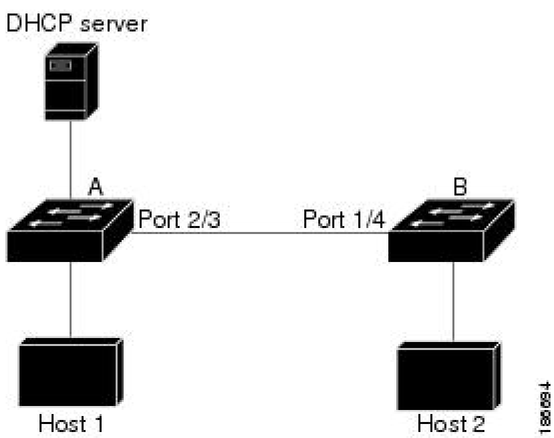
Configuration Examples for DAI

Example 1-Two Devices Support DAI

These procedures show how to configure DAI when two devices support DAI.

Figure 26: Two Devices Supporting DAI

The following figure shows the network configuration for this example. Host 1 is connected to device A, and Host 2 is connected to device B. Both devices are running DAI on VLAN 1 where the hosts are located. A DHCP server is connected to device A. Both hosts acquire their IP addresses from the same DHCP server. Device A has the bindings for Host 1 and Host 2, and device B has the binding for Host 2. Device A Ethernet interface 2/3 is connected to the device B Ethernet interface 1/4.



DAI depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically-assigned IP addresses.

- This configuration does not work if the DHCP server is moved from device A to a different location.
- To ensure that this configuration does not compromise security, configure Ethernet interface 2/3 on device A and Ethernet interface 1/4 on device B as trusted.

Configuring Device A

To enable DAI and configure Ethernet interface 2/3 on device A as trusted, follow these steps:

Step 1 While logged into device A, verify the connection between device A and device B.

```
switchA# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
switchB                Ethernet2/3     177     R S I    WS-C2960-24TC Ethernet1/4
switchA#
```

Step 2 Enable DAI on VLAN 1 and verify the configuration.

```
switchA# config t
switchA(config)# ip arp inspection vlan 1
switchA(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----------
Configuration   : Enabled
Operation State : Active
switchA(config)#
```

Step 3 Configure Ethernet interface 2/3 as trusted.

```
switchA(config)# interface ethernet 2/3
switchA(config-if)# ip arp inspection trust
switchA(config-if)# exit
switchA(config)# exit
switchA# show ip arp inspection interface ethernet 2/3
 Interface        Trust State    Rate (pps)    Burst Interval
 -------------    -----------    ----------    --------------
 Ethernet2/3      Trusted           15             5
```

Step 4 Verify the bindings.

```
switchA# show ip dhcp snooping binding
MacAddress         IpAddress        LeaseSec  Type           VLAN  Interface
-----------------  ---------------  --------  -------------  ----  -------------
00:60:0b:00:12:89  10.0.0.1         0         dhcp-snooping  1     Ethernet2/3
switchA#
```

Step 5 Check the statistics before and after DAI processes any packets.

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
```

```
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

If host 1 sends out two ARP requests with an IP address of 10.0.0.1 and a MAC address of 0002.0002.0002, both requests are permitted, and are shown as follows:

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
```

If host 1 tries to send an ARP request with an IP address of 10.0.0.3, the packet is dropped and an error message is logged.

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Ethernet2/3, vlan
1.([0002.0002.0002/10.0.0.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Fri Jul 13 2008])
```

The statistics display as follows:

```
switchA# show ip arp inspection statistics vlan 1
switchA#
Vlan : 1
-----------
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 2
ARP Res Dropped    = 0
DHCP Drops         = 2
DHCP Permits       = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

Configuring Device B

To enable DAI and configure Ethernet interface 1/4 on device B as trusted, follow these steps:

Step 1 While logged into device B, verify the connection between device B and device A.

```
switchB# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
```

```
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
switchA                Ethernet1/4     120     R S I    WS-C2960-24TC Ethernet2/3
switchB#
```

Step 2 Enable DAI on VLAN 1, and verify the configuration.

```
switchB# config t
switchB(config)# ip arp inspection vlan 1
switchB(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----------
Configuration    : Enabled
Operation State : Active
switchB(config)#
```

Step 3 Configure Ethernet interface 1/4 as trusted.

```
switchB(config)# interface ethernet 1/4
switchB(config-if)# ip arp inspection trust
switchB(config-if)# exit
switchB(config)# exit
switchB# show ip arp inspection interface ethernet 1/4
 Interface        Trust State    Rate (pps)    Burst Interval
 -------------    -----------    ----------    --------------
 Ethernet1/4      Trusted           15            5
switchB#
```

Step 4 Verify the list of DHCP snooping bindings.

```
switchB# show ip dhcp snooping binding
MacAddress         IpAddress        LeaseSec  Type           VLAN  Interface
-----------------  ---------------  --------  -------------  ----  -------------
00:01:00:01:00:01  10.0.0.2         4995      dhcp-snooping  1     Ethernet1/4
switchB#
```

Step 5 Check the statistics before and after DAI processes any packets.

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

If Host 2 sends out an ARP request with the IP address 10.0.0.2 and the MAC address 0001.0001.0001, the packet is forwarded and the statistics are updated.

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 1
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

If Host 2 attempts to send an ARP request with the IP address 10.0.0.1, DAI drops the request and logs the following system message:

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Ethernet1/4, vlan
1.([0001.0001.0001/10.0.0.1/0000.0000.0000/0.0.0.0/01:53:21 UTC Fri Jun 13 2008])
```

The statistics display as follows:

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 1
ARP Res Forwarded  = 0
ARP Req Dropped    = 1
ARP Res Dropped    = 0
DHCP Drops         = 1
DHCP Permits       = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

Example 2 One Device Supports DAI

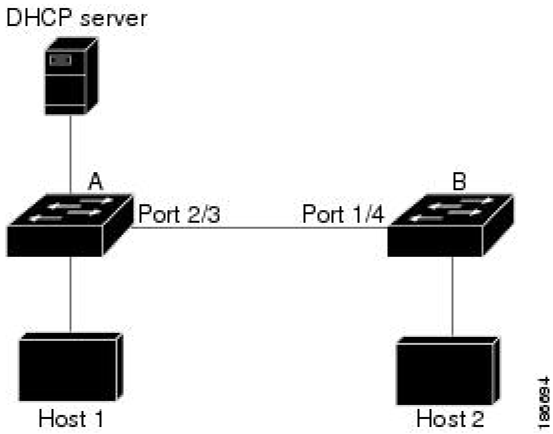
This procedure shows how to configure DAI when the second device involved in the network configuration does not support DAI or DHCP snooping.

Figure 27: One Device Supporting DAI

Device B, shown in this figure does not support DAI or DHCP snooping; therefore, configuring Ethernet interface 2/3 on device A as trusted creates a security hole because both device A and Host 1 could be attacked by either device B or Host 2.

To prevent this possibility, you must configure Ethernet interface 2/3 on device A as untrusted. To permit ARP packets from Host 2, you must set up an ARP ACL and apply it to VLAN 1. If the IP address of Host

2 is not static, which would make it impossible to accurately configure the ARP ACL on device A, you must separate device A from device B at Layer 3 and use a router to route packets between them.



Step 1 Configure the access list to permit the IP address 10.0.0.1 and the MAC address 0001.0001.0001, and verify the configuration.

```
switchA# config t
switchA(config)# arp access-list H2
switchA(config-arp-acl)# permit ip host 10.0.0.1 mac host 0001.0001.0001
switchA(config-arp-acl)# exit
switchA(config)# show arp access-lists H2
ARP access list H2
10 permit ip host 1.1.1.1 mac host 0001.0001.0001
switchA(config)#
```

Step 2 Apply the ACL to VLAN 1, and verify the configuration.

```
switchA(config)# ip arp inspection filter H2 vlan 1
switchA(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 200
-----------
Configuration    : Enabled
Operation State  : Active
ACL Match/Static : H2 / No
```

Step 3 Configure Ethernet interface 2/3 as untrusted, and verify the configuration.

Note By default, the interface is untrusted.

```
switchA(config)# interface ethernet 2/3
switchA(config-if)# no ip arp inspection trust
switchA(config-if)# exit
switchA# show ip arp inspection interface ethernet 2/3
switchA#
```

The **show ip arp inspection interface** command has no output because the interface has the default configuration, which includes an untrusted state.

When Host 2 sends 5 ARP requests through Ethernet interface 2/3 on device A and a "get" is permitted by device A, the statistics are updated.

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 5
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

Configuring ARP ACLs

Session Manager Support for ARP ACLs

Session Manager supports the configuration of ARP ACLs. This feature allows you to create a configuration session and verify your ARP ACL 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 an ARP ACL

You can create an ARP ACL on the device and add rules to it.

SUMMARY STEPS

1. **configure terminal**
2. **arp access-list** *name*
3. [*sequence-number*] {**permit** | **deny**} **ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]
4. [*sequence-number*] {**permit** | **deny**} **request ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]
5. [*sequence-number*] {**permit** | **deny**} **response ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} [**any** | **host** *target-IP* | *target-IP target-IP-mask*]] **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**any** | **host** *target-MAC* | *target-MAC target-MAC-mask*] [**log**]
6. (Optional) **show arp access-lists** *acl-name*
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**arp access-list** *name*
	Example:
	`switch(config)# arp access-list arp-acl-01`
	`switch(config-arp-acl)#`
		Creates the ARP ACL and enters ARP ACL configuration mode.

Step 3	[*sequence-number*] {**permit** | **deny**} **ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**] **Example:** `switch(config-arp-acl)# permit ip 192.168.2.0 255.2555.255.0 mac 00C0.4F00.0000 ffff.ff00.0000`	Creates a rule that permits or denies any ARP message based upon the IP address and MAC address of the sender of the message. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the rules.
Step 4	[*sequence-number*] {**permit** | **deny**} **request ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**] **Example:** `switch(config-arp-acl)# permit request ip 192.168.102.0 0.0.0.255 mac any`	Creates a rule that permits or denies ARP request messages based upon the IP address and MAC address of the sender of the message. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the rules.
Step 5	[*sequence-number*] {**permit** | **deny**} **response ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} [**any** | **host** *target-IP* | *target-IP target-IP-mask*]] **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**any** | **host** *target-MAC* | *target-MAC target-MAC-mask*] [**log**] **Example:** `switch(config-arp-acl)# permit response ip host 192.168.202.32 any mac host 00C0.4FA9.BCF3 any`	Creates a rule that permits or denies ARP response messages based upon the IPv4 address and MAC address of the sender and the target of the message. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the rules.
Step 6	(Optional) **show arp access-lists** *acl-name* **Example:** `switch(config-arp-acl)# show arp access-lists arp-acl-01`	Shows the ARP ACL configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config-arp-acl)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Changing an ARP ACL

You can change and remove rules in an existing ARP 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.

SUMMARY STEPS

1. **configure terminal**
2. **arp access-list** *name*
3. (Optional) [*sequence-number*] {**permit** | **deny**} [**request** | **response**] **ip** *IP-data* **mac** *MAC-data*
4. (Optional) **no** {*sequence-number* | {**permit** | **deny**} [**request** | **response**] **ip** *IP-data* **mac** *MAC-data*
5. **show arp access-lists**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**arp access-list** *name*
	Example:
	`switch(config)# arp access-list arp-acl-01`
	`switch(config-acl)#`
		Enters ARP ACL configuration mode for the ACL that you specify by name.

Step 3	(Optional) [*sequence-number*] {**permit** | **deny**} [**request** | **response**] **ip** *IP-data* **mac** *MAC-data* **Example:** `switch(config-arp-acl)# 100 permit request ip 192.168.132.0 255.2555.255.0 mac any`	Creates a rule. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the rules.
Step 4	(Optional) **no** {*sequence-number* | {**permit** | **deny**} [**request** | **response**] **ip** *IP-data* **mac** *MAC-data* **Example:** `switch(config-arp-acl)# no 80`	Removes the rule that you specified from the ARP ACL.
Step 5	**show arp access-lists** **Example:** `switch(config-arp-acl)# show arp access-lists`	Displays the ARP ACL configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:**	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	`switch(config-arp-acl)# copy running-config startup-config`	

Related Topics

Creating an ARP ACL, on page 570
Changing Sequence Numbers in an ARP ACL, on page 574

Removing an ARP ACL

You can remove an ARP ACL from the device.

Before you begin

Ensure that you know whether the ACL is applied to a VLAN. The device allows you to remove ACLs that are currently applied. Removing an ACL does not affect the configuration of VLANs where you have applied the ACL. Instead, the device considers the removed ACL to be empty.

SUMMARY STEPS

1. **configure terminal**
2. **no arp access-list** *name*
3. **show arp access-lists**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no arp access-list** *name* **Example:** `switch(config)# no arp access-list arp-acl-01`	Removes the ARP ACL you specified by name from running configuration.
Step 3	**show arp access-lists** **Example:** `switch(config)# show arp access-lists`	Displays the ARP ACL 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.

Changing Sequence Numbers in an ARP ACL

You can change all the sequence numbers assigned to rules in an ARP ACL.

SUMMARY STEPS

1. **configure terminal**
2. **resequence arp access-list** *name starting-sequence-number increment*
3. **show arp access-lists** *name*
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**resequence arp access-list** *name starting-sequence-number increment*
	Example:
	`switch(config)# resequence arp access-list arp-acl-01 100 10`
	`switch(config)#`
		Assigns sequence numbers to the rules contained in the ACL, where the first rule receives the starting sequence number that you specify. Each subsequent rule receives a number larger than the preceding rule. The difference in numbers is determined by the increment that you specify.

Step 3	**show arp access-lists** *name* **Example:** `switch(config)# show arp access-lists arp-acl-01`	Displays the ARP ACL configuration for the ACL specified by the *name* argument.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the ARP ACL Configuration

To display ARP ACL configuration information, use the commands in this table. For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
show arp access-lists	Displays the ARP ACL configuration.
show running-config aclmgr	Displays ACLs in the running configuration.

Additional References for DAI

Related Documents

Related Topic	Document Title
DAI commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference*
DHCP snooping commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

Standards

Standards	Title
RFC-826	An Ethernet Address Resolution Protocol

Feature History for DAI

This table lists the release history for this feature.

Table 39: Feature History for DAI

Feature Name	Releases	Feature Information	
Dynamic ARP Inspection	6.0(1)	No change from Release 5.2.	
Dynamic ARP Inspection	5.2(1)	No change from Release 5.1.	
Dynamic ARP Inspection	5.1(1)	No change from Release 5.0.	
Dynamic ARP Inspection	5.0(2)	No change from Release 4.2.	
Dynamic ARP Inspection	4.2(1)	No change from Release 4.1.	

CHAPTER 20

Configuring IP Source Guard

This chapter describes how to configure IP Source Guard on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About IP Source Guard

IP Source Guard is a per-interface traffic filter that permits IP traffic only when the IP address and MAC address of each packet matches one of two sources of IP and MAC address bindings:

- Entries in the Dynamic Host Configuration Protocol (DHCP) snooping binding table.
- Static IP source entries that you configure.

Filtering on trusted IP and MAC address bindings helps prevent spoofing attacks, in which an attacker uses the IP address of a valid host to gain unauthorized network access. To circumvent IP Source Guard, an attacker would have to spoof both the IP address and the MAC address of a valid host.

You can enable IP Source Guard on Layer 2 interfaces that are not trusted by DHCP snooping. IP Source Guard supports interfaces that are configured to operate in access mode and trunk mode. When you initially enable IP Source Guard, all inbound IP traffic on the interface is blocked except for the following:

- DHCP packets, which DHCP snooping inspects and then forwards or drops, depending upon the results of inspecting the packet.
- IP traffic from static IP source entries that you have configured in the Cisco NX-OS device.

The device permits the IP traffic when DHCP snooping adds a binding table entry for the IP address and MAC address of an IP packet or when you have configured a static IP source entry.

The device drops IP packets when the IP address and MAC address of the packet do not have a binding table entry or a static IP source entry. For example, assume that the **show ip dhcp snooping binding** command displays the following binding table entry:

```
MacAddress          IpAddress     LeaseSec   Type         VLAN      Interface
----------          ----------    ---------  ------       -------    ---------
00:02:B3:3F:3B:99   10.5.5.2        6943    dhcp-snooping  10       Ethernet2/3
```

If the device receives an IP packet with an IP address of 10.5.5.2, IP Source Guard forwards the packet only if the MAC address of the packet is 00:02:B3:3F:3B:99.

Virtualization Support for IP Source Guard

The following information applies to IP Source Guard used in virtual device contexts (VDCs):

- IP-MAC address bindings are unique per VDC. Bindings in one VDC do not affect IP Source Guard in other VDCs.
- Cisco NX-OS does not limit the binding database size on a per-VDC basis.

Prerequisites for IP Source Guard

IP Source Guard has the following prerequisite:

- You must enable the DHCP feature.

Guidelines and Limitations for IP Source Guard

IP Source Guard has the following configuration guidelines and limitations:

- IP Source Guard limits IP traffic on an interface to only those sources that have an IP-MAC address binding table entry or static IP source entry. When you first enable IP Source Guard on an interface, you may experience disruption in IP traffic until the hosts on the interface receive a new IP address from a DHCP server.
- IP Source Guard is dependent upon DHCP snooping to build and maintain the IP-MAC address binding table or upon manual maintenance of static IP source entries.

Default Settings for IP Source Guard

This table lists the default settings for IP Source Guard parameters.

Table 40: Default IP Source Guard Parameters

Parameters	Default
IP Source Guard	Disabled on each interface.
IP source entries	None. No static or default IP source entries exist by default.

Configuring IP Source Guard

Enabling or Disabling IP Source Guard on a Layer 2 Interface

You can enable or disable IP Source Guard on a Layer 2 interface. By default, IP Source Guard is disabled on all interfaces.

Before you begin

Ensure that the DHCP feature is enabled.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. [**no**] **ip verify source dhcp-snooping-vlan**
4. (Optional) **show running-config dhcp**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot*/*port*
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		Enters interface configuration mode for the specified interface.

Step 3	[**no**] **ip verify source dhcp-snooping-vlan** **Example:**	Enables IP Source Guard on the interface. The **no** option disables IP Source Guard on the interface.

	Command or Action	Purpose
	`switch(config-if)# ip verify source dhcp-snooping vlan`	
Step 4	(Optional) **show running-config dhcp** **Example:** `switch(config-if)# show running-config dhcp`	Displays the running configuration for DHCP snooping, including the IP Source Guard configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Adding or Removing a Static IP Source Entry, on page 580

Adding or Removing a Static IP Source Entry

You can add or remove a static IP source entry on a device. By default, there are no static IP source entries on a device.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ip source binding** *IP-address* *MAC-address* **vlan** *vlan-ID* **interface ethernet** *slot*/*port*
3. (Optional) **show ip dhcp snooping binding** [**interface ethernet** *slot*/*port*]
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip source binding** *IP-address* *MAC-address* **vlan** *vlan-ID* **interface ethernet** *slot*/*port* **Example:** `switch(config)# ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3`	Creates a static IP source entry for the current interface, or if you use the **no** option, removes a static IP source entry.
Step 3	(Optional) **show ip dhcp snooping binding** [**interface ethernet** *slot*/*port*] **Example:** `switch(config)# show ip dhcp snooping binding interface ethernet 2/3`	Displays IP-MAC address bindings for the interface specified, including static IP source entries. Static entries appear with the term in the Type column.

	Command or Action	Purpose
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling or Disabling IP Source Guard on a Layer 2 Interface, on page 579
Displaying IP Source Guard Bindings, on page 581

Displaying IP Source Guard Bindings

Use the **show ip verify source** command to display IP-MAC address bindings.

Configuration Example for IP Source Guard

This example shows how to create a static IP source entry and then how to enable IP Source Guard on an interface.

```
ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3
interface ethernet 2/3
  no shutdown
  ip verify source dhcp-snooping-vlan
```

Additional References for IP Source Guard

Related Documents

Related Topic	Document Title
IP Source Guard commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for IP Source Guard

This table lists the release history for this feature.

Table 41: Feature History for IP Source Guard

Feature Name	Releases	Feature Information	
IP Source Guard	6.0(1)	No change from Release 5.2.	
IP Source Guard	5.2(1)	No change from Release 5.1.	
IP Source Guard	5.1(1)	No change from Release 5.0.	
IP Source Guard	5.0(2)	No change from Release 4.2.	
IP Source Guard	4.2(1)	No change from Release 4.1.	

CHAPTER 21

Configuring Password Encryption

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

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Password Encryption

This section includes information about password encryption on Cisco NX-OS devices.

AES Password Encryption and Master Encryption Keys

You can enable strong, reversible 128-bit Advanced Encryption Standard (AES) password encryption, also known as type-6 encryption. To start using type-6 encryption, you must enable the AES password encryption feature and configure a master encryption key, which is used to encrypt and decrypt passwords.

After you enable AES password encryption and configure a master key, all existing and newly created clear-text passwords for supported applications (currently RADIUS and TACACS+) are stored in type-6 encrypted format, unless you disable type-6 password encryption. You can also configure Cisco NX-OS to convert all existing weakly encrypted passwords to type-6 encrypted passwords.

Related Topics

Configuring a Master Key and Enabling the AES Password Encryption Feature, on page 43
Configuring Global RADIUS Keys, on page 69
Configuring a Key for a Specific RADIUS Server, on page 71
Configuring Global TACACS+ Keys, on page 102
Configuring a Key for a Specific TACACS+ Server, on page 103

Virtualization Support for Password Encryption

The master key used with the AES password encryption feature is unique for each VDC.

Note For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Licensing Requirements for Password Encryption

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	Password encryption 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 an explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Guidelines and Limitations for Password Encryption

Password encryption has the following configuration guidelines and limitations:

- Only users with administrator privilege (network-admin or vdc-admin) can configure the AES password encryption feature, associated encryption and decryption commands, and master keys.
- RADIUS and TACACS+ are the only applications that can use the AES password encryption feature.
- Configurations containing type-6 encrypted passwords are not rollback compliant.
- You can enable the AES password encryption feature without a master key, but encryption starts only when a master key is present in the system.
- Deleting the master key stops type-6 encryption and causes all existing type-6 encrypted passwords to become unusable, unless the same master key is reconfigured.
- Before you downgrade from Cisco NX-OS Release 5.2 to an earlier release, decrypt all type-6 passwords, disable the AES password encryption feature, and delete the master key.

- To move the device configuration to another device, either decrypt the configuration before porting it to the other device or configure the same master key on the device to which the configuration will be applied.

Default Settings for Password Encryption

This table lists the default settings for password encryption parameters.

Table 42: Default Password Encryption Parameter Settings

Parameters	Default
AES password encryption feature	Disabled
Master key	Not configured

Configuring Password Encryption

This section describes the tasks for configuring password encryption on Cisco NX-OS devices.

Note 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.

Configuring a Master Key and Enabling the AES Password Encryption Feature

You can configure a master key for type-6 encryption and enable the Advanced Encryption Standard (AES) password encryption feature.

SUMMARY STEPS

1. [**no**] **key config-key ascii**
2. **configure terminal**
3. [**no**] **feature password encryption aes**
4. (Optional) **show encryption service stat**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	[**no**] **key config-key ascii**
	Example:
	`switch# key config-key ascii`
	`New Master Key:`
	`Retype Master Key:`
		Configures a master key to be used with the AES password encryption feature. The master key can contain between 16 and 32 alphanumeric characters. You can use the **no** form of this command to delete the master key at any time.
		If you enable the AES password encryption feature before configuring a master key, a message appears stating that

	Command or Action	Purpose
		password encryption will not take place unless a master key is configured. If a master key is already configured, you are prompted to enter the current master key before entering a new master key.

Step 2	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 3	[**no**] **feature password encryption aes** **Example:** `switch(config)# feature password encryption aes`	Enables or disables the AES password encryption feature.
Step 4	(Optional) **show encryption service stat** **Example:** `switch(config)# show encryption service stat`	Displays the configuration status of the AES password encryption feature and the master key.
Step 5	Required: **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration. **Note** This command is necessary to synchronize the master key in the running configuration and the startup configuration.

Related Topics

Configuring Text for a Key, on page 596
Configuring Accept and Send Lifetimes for a Key, on page 598
AES Password Encryption and Master Encryption Keys, on page 30

Converting Existing Passwords to Type-6 Encrypted Passwords

You can convert existing plain or weakly encrypted passwords to type-6 encrypted passwords.

Before you begin

Ensure that you have enabled the AES password encryption feature and configured a master key.

SUMMARY STEPS

1. **encryption re-encrypt obfuscated**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**encryption re-encrypt obfuscated** **Example:**	Converts existing plain or weakly encrypted passwords to type-6 encrypted passwords.

	Command or Action	Purpose
	`switch# encryption re-encrypt obfuscated`	

Converting Type-6 Encrypted Passwords Back to Their Original States

You can convert type-6 encrypted passwords back to their original states.

Before you begin

Ensure that you have configured a master key.

SUMMARY STEPS

1. **encryption decrypt type6**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**encryption decrypt type6**
	Example:
	`switch# encryption decrypt type6`
	`Please enter current Master Key:`
		Converts type-6 encrypted passwords back to their original states.

Deleting Type-6 Encrypted Passwords

You can delete all type-6 encrypted passwords from the Cisco NX-OS device.

SUMMARY STEPS

1. **encryption delete type6**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**encryption delete type6** **Example:** `switch# encryption delete type6`	Deletes all type-6 encrypted passwords.

Verifying the Password Encryption Configuration

To display password encryption configuration information, perform the following task:

Command	Purpose
show encryption service stat	Displays the configuration status of the AES password encryption feature and the master key.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuration Examples for Password Encryption

The following example shows how to create a master key, enable the AES password encryption feature, and configure a type-6 encrypted password for a TACACS+ application:

```
key config-key ascii
  New Master Key:
  Retype Master Key:
configure terminal
feature password encryption aes
show encryption service stat
  Encryption service is enabled.
  Master Encryption Key is configured.
  Type-6 encryption is being used.
feature tacacs+
tacacs-server key Cisco123
show running-config tacacs+
  feature tacacs+
  logging level tacacs 5
  tacacs-server key 6
"JDYkqyIFWeBvzpljSfWmRZrmRSRE8syxKlOSjP9RCCkFinZbJI3GD5c6rckJR/Qju2PKLmOewbheAA=="
```

Additional References for Password Encryption

This section includes additional information related to implementing password encryption.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for Password Encryption

This table lists the release history for this feature.

Table 43: Feature History for Password Encryption

Feature Name	Releases	Feature Information
Password encryption	6.0(1)	No change from Release 5.2.
Password encryption	5.2(1)	This feature was introduced.

CHAPTER 22

Configuring Keychain Management

This chapter describes how to configure keychain management on a Cisco NX-OS device.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Keychain Management

Keychains and Keychain Management

Keychain management allows you to create and maintain keychains, which are sequences of keys (sometimes called shared secrets). You can use keychains with features that secure communications with other devices by using key-based authentication. The device allows you to configure multiple keychains.

Some routing protocols that support key-based authentication can use a keychain to implement a hitless key rollover for authentication. For more information, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

Lifetime of a Key

To maintain stable communications, each device that uses a protocol that is secured by key-based authentication must be able to store and use more than one key for a feature at the same time. Based on the send and accept lifetimes of a key, keychain management provides a secure mechanism to handle key rollover. The device uses the lifetimes of keys to determine which keys in a keychain are active.

Each key in a keychain has two lifetimes, as follows:

Accept lifetime

The time interval within which the device accepts the key during a key exchange with another device.

Send lifetime

The time interval within which the device sends the key during a key exchange with another device.

You define the send and accept lifetimes of a key using the following parameters:

Start-time

The absolute time that the lifetime begins.

End-time

The end time can be defined in one of the following ways:

- The absolute time that the lifetime ends
- The number of seconds after the start time that the lifetime ends
- Infinite lifetime (no end-time)

During a key send lifetime, the device sends routing update packets with the key. The device does not accept communication from other devices when the key sent is not within the accept lifetime of the key on the device.

We recommend that you configure key lifetimes that overlap within every keychain. This practice avoids failure of neighbor authentication due to the absence of active keys.

Virtualization Support for Keychain Management

The following information applies to keychains used in virtual device contexts (VDCs):

- Keychains are unique per VDC. You cannot use a keychain that you created in one VDC in a different VDC.
- Because keychains are not shared by VDCs, you can reuse keychain names in different VDCs.
- The device does not limit keychains on a per-VDC basis.

Licensing Requirements for Keychain Management

This table shows the licensing requirements for keychain management.

Product	License Requirement
Cisco NX-OS	Keychain management 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 an explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Prerequisites for Keychain Management

Keychain management has no prerequisites.

Guidelines and Limitations for Keychain Management

Keychain management has the following configuration guideline and limitation:

- Changing the system clock impacts when the keys are active.

Default Settings for Keychain Management

This table lists the default settings for Cisco NX-OS keychain management parameters.

Table 44: Default Keychain Management Parameters

Parameters	Default
Key chains	No keychain exists by default.
Keys	No keys are created by default when you create a new keychain.
Accept lifetime	Always valid.
Send lifetime	Always valid.
Key-string entry encryption	Unencrypted.

Configuring Keychain Management

Creating a Keychain

You can create a keychain on the device. A new keychain contains no keys.

SUMMARY STEPS

1. **configure terminal**
2. **key chain** *name*
3. (Optional) **show key chain** *name*
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**key chain** *name*
	Example:
	`switch(config)# key chain glbp-keys`
	`switch(config-keychain)#`
		Creates the keychain and enters keychain configuration mode.

Step 3	(Optional) **show key chain** *name* **Example:** `switch(config-keychain)# show key chain glbp-keys`	Displays the keychain configuration.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-keychain)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring a Master Key and Enabling the AES Password Encryption Feature, on page 43

Removing a Keychain

You can remove a keychain on the device.

Note Removing a keychain removes any keys within the keychain.

Before you begin

If you are removing a keychain, ensure that no feature uses it. If a feature is configured to use a keychain that you remove, that feature is likely to fail to communicate with other devices.

SUMMARY STEPS

1. **configure terminal**

2. **no key chain** *name*
3. (Optional) **show key chain** *name*
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no key chain** *name* **Example:** `switch(config)# no key chain glbp-keys`	Removes the keychain and any keys that the keychain contains.
Step 3	(Optional) **show key chain** *name* **Example:** `switch(config-keychain)# show key chain glbp-keys`	Confirms that the keychain no longer exists in running configuration.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-keychain)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Creating a Keychain, on page 593

Configuring a Master Key and Enabling the AES Password Encryption Feature

You can configure a master key for type-6 encryption and enable the Advanced Encryption Standard (AES) password encryption feature.

SUMMARY STEPS

1. [**no**] **key config-key ascii**
2. **configure terminal**
3. [**no**] **feature password encryption aes**
4. (Optional) **show encryption service stat**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	[**no**] **key config-key ascii** **Example:**	Configures a master key to be used with the AES password encryption feature. The master key can contain between 16

	Command or Action	Purpose

	`switch# key config-key ascii`
	`New Master Key:`
	`Retype Master Key:`
		and 32 alphanumeric characters. You can use the **no** form of this command to delete the master key at any time.
		
		If you enable the AES password encryption feature before configuring a master key, a message appears stating that password encryption will not take place unless a master key is configured. If a master key is already configured, you are prompted to enter the current master key before entering a new master key.

Step 2	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 3	[**no**] **feature password encryption aes** **Example:** `switch(config)# feature password encryption aes`	Enables or disables the AES password encryption feature.
Step 4	(Optional) **show encryption service stat** **Example:** `switch(config)# show encryption service stat`	Displays the configuration status of the AES password encryption feature and the master key.
Step 5	Required: **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration. **Note** This command is necessary to synchronize the master key in the running configuration and the startup configuration.

Related Topics

Configuring Text for a Key, on page 596
Configuring Accept and Send Lifetimes for a Key, on page 598
AES Password Encryption and Master Encryption Keys, on page 30

Configuring Text for a Key

You can configure the text for a key. The text is the shared secret. The device stores the text in a secure format.

By default, accept and send lifetimes for a key are infinite, which means that the key is always valid. After you configure the text for a key, configure the accept and send lifetimes for the key.

Before you begin

Determine the text for the key. You can enter the text as unencrypted text or in the encrypted form that Cisco NX-OS uses to display key text when you use the **show key chain** command. Using the encrypted form is particularly helpful if you are creating key text to match a key as shown in the **show key chain** command output from another device.

SUMMARY STEPS

1. **configure terminal**
2. **key chain** *name*
3. **key** *key-ID*
4. **key-string** [*encryption-type*] *text-string*
5. (Optional) **show key chain** *name* [**mode decrypt**]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**key chain** *name*
	Example:
	`switch(config)# key chain glbp-keys`
	`switch(config-keychain)#`
		Enters keychain configuration mode for the keychain that you specified.

Step 3	**key** *key-ID*
	Example:
	`switch(config-keychain)# key 13`
	`switch(config-keychain-key)#`
		Enters key configuration mode for the key that you specified. The *key-ID* argument must be a whole number between 0 and 65535.

Step 4	**key-string** [*encryption-type*] *text-string* **Example:** `switch(config-keychain-key)# key-string 0 AS3cureStr1ng`	Configures the text string for the key. The *text-string* argument is alphanumeric, case-sensitive, and supports special characters. The *encryption-type* argument can be one of the following values: • 0—The *text-string* argument that you enter is unencrypted text. This is the default. • 7—The *text-string* argument that you enter is encrypted. The encryption method is a Cisco proprietary method. This option is useful when you are entering a text string based on the encrypted output of a **show key chain** command that you ran on another Cisco NX-OS device. The value of the first 2 digits of a type 7 key string configured by using the **key-string 7** *text-string* command has to be between 0 and 15. For example, you can configure 07372b557e2c1a as the key string value in which case the sum value of the first 2 digits will be 7. But, you cannot configure 85782916342021 as the key string value because the value of the first 2 digits will be 85. We recommend

	Command or Action	Purpose
		unconfiguring any type 7 key strings that do not adhere to this value or to configure a type 0 string.
Step 5	(Optional) **show key chain** *name* [**mode decrypt**] **Example:** `switch(config-keychain-key)# show key chain glbp-keys`	Shows the keychain configuration, including the key text configuration. The mode decrypt option, which can be used by a device administrator only, displays the keys in cleartext.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-keychain-key)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring Accept and Send Lifetimes for a Key, on page 598

Configuring Accept and Send Lifetimes for a Key

You can configure the accept lifetime and send lifetime for a key. By default, accept and send lifetimes for a key are infinite, which means that the key is always valid.

Note We recommend that you configure the keys in a keychain to have overlapping lifetimes. This practice prevents loss of key-secured communication due to moments where no key is active.

SUMMARY STEPS

1. **configure terminal**
2. **key chain** *name*
3. **key** *key-ID*
4. **accept-lifetime** [**local**] *start-time* **duration** *duration-value* | **infinite** | *end-time*]
5. **send-lifetime** [**local**] *start-time* **duration** *duration-value* | **infinite** | *end-time*]
6. (Optional) **show key chain** *name* [**mode decrypt**]
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**key chain** *name*
	Example:
	`switch(config)# key chain glbp-keys`
	`switch(config-keychain)#`
		Enters keychain configuration mode for the keychain that you specified.

Step 3	**key** *key-ID*
	Example:
	`switch(config-keychain)# key 13`
	`switch(config-keychain-key)#`
		Enters key configuration mode for the key that you specified.

Step 4	**accept-lifetime** [**local**] *start-time* **duration** *duration-value* | **infinite** | *end-time*] **Example:** `switch(config-keychain-key)# accept-lifetime 00:00:00 Jun 13 2008 23:59:59 Sep 12 2008`	Configures an accept lifetime for the key. By default, the device treats the *start-time* and *end-time* arguments as UTC. If you specify the **local** keyword, the device treats these times as local times. The *start-time* argument is the time of day and date that the key becomes active. Specify the end of the lifetime with one of the following options: • **duration** *duration-value* —The length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years). • **infinite**—The accept lifetime of the key never expires. • *end-time* —The *end-time* argument is the time of day and date that the key becomes inactive.
Step 5	**send-lifetime** [**local**] *start-time* **duration** *duration-value* | **infinite** | *end-time*] **Example:** `switch(config-keychain-key)# send-lifetime 00:00:00 Jun 13 2008 23:59:59 Aug 12 2008`	Configures a send lifetime for the key. By default, the device treats the *start-time* and *end-time* arguments as UTC. If you specify the **local** keyword, the device treats these times as local times. The *start-time* argument is the time of day and date that the key becomes active. You can specify the end of the send lifetime with one of the following options: • **duration** *duration-value* —The length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years). • **infinite**—The send lifetime of the key never expires. • *end-time* —The *end-time* argument is the time of day and date that the key becomes inactive.
Step 6	(Optional) **show key chain** *name* [**mode decrypt**] **Example:**	Shows the keychain configuration, including the key text configuration. The mode decrypt option, which can be used

	Command or Action	Purpose
	`switch(config-keychain-key)# show key chain glbp-keys`	by a device administrator only, displays the keys in cleartext.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config-keychain-key)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Lifetime of a Key, on page 592

Determining Active Key Lifetimes

To determine which keys within a keychain have active accept or send lifetimes, use the command in this table. For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
show key chain	Displays the keychains configured on the device.

Verifying the Keychain Management Configuration

To display keychain management configuration information, perform the following task. For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
show key chain	Displays the keychains configured on the device.

Configuration Example for Keychain Management

This example shows how to configure a keychain named glbp keys. Each key text string is encrypted. Each key has longer accept lifetimes than send lifetimes, to help prevent lost communications by accidentally configuring a time in which there are no active keys.

```
key chain glbp-keys
  key 0
    key-string 7 zqdest
    accept-lifetime 00:00:00 Jun 01 2008 23:59:59 Sep 12 2008
    send-lifetime 00:00:00 Jun 01 2008 23:59:59 Aug 12 2008
  key 1
    key-string 7 uaeqdyito
    accept-lifetime 00:00:00 Aug 12 2008 23:59:59 Dec 12 2008
    send-lifetime 00:00:00 Sep 12 2008 23:59:59 Nov 12 2008
```

```
key 2
  key-string 7 eekgsdyd
  accept-lifetime 00:00:00 Nov 12 2008 23:59:59 Mar 12 2009
  send-lifetime 00:00:00 Dec 12 2008 23:59:59 Feb 12 2009
```

Where to Go Next

For information about routing features that use keychains, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

Additional References for Keychain Management

Related Documents

Related Topic	Document Title
Gateway Load Balancing Protocol	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*
Border Gateway Protocol	*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*
Keychain management commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

CHAPTER 23

Configuring Traffic Storm Control

This chapter describes how to configure traffic storm control on the Cisco NX-OS device.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

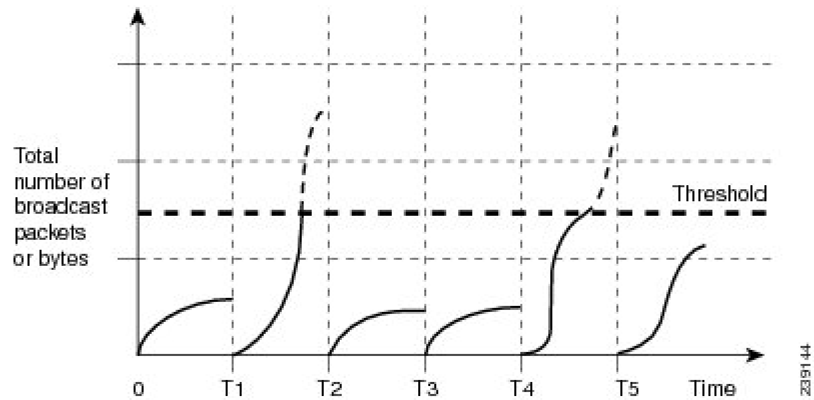
Information About Traffic Storm Control

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. You can use the traffic storm control feature to prevent disruptions on Layer 2 ports by a broadcast, multicast, or unicast traffic storm on physical interfaces.

Traffic storm control (also called traffic suppression) allows you to monitor the levels of the incoming broadcast, multicast, and unicast traffic over a 10-millisecond interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.

This table shows the broadcast traffic patterns on a Layer 2 interface over a given interval. In this example, traffic storm control occurs between times T1 and T2 and between T4 and T5. During those intervals, the amount of broadcast traffic exceeded the configured threshold.

Figure 28: Broadcast Suppression



The traffic storm control threshold numbers and the time interval allow the traffic storm control algorithm to work with different levels of granularity. A higher threshold allows more packets to pass through.

Traffic storm control on the Cisco NX-OS device is implemented in the hardware. The traffic storm control circuitry monitors packets that pass from a Layer 2 interface to the switching bus. Using the Individual/Group bit in the packet destination address, the circuitry determines if the packet is unicast or broadcast, tracks the current count of packets within the 10-millisecond interval, and filters out subsequent packets when a threshold is reached.

Traffic storm control uses a bandwidth-based method to measure traffic. You set the percentage of total available bandwidth that the controlled traffic can use. Because packets do not arrive at uniform intervals, the 10-millisecond interval can affect the behavior of traffic storm control.

The following are examples of traffic storm control behavior:

- If you enable broadcast traffic storm control, and broadcast traffic exceeds the level within the 10-millisecond interval, traffic storm control drops all broadcast traffic until the end of the interval.
- If you enable broadcast and multicast traffic storm control, and the combined broadcast and multicast traffic exceeds the level within the 10-millisecond interval, traffic storm control drops all broadcast and multicast traffic until the end of the interval.
- If you enable broadcast and multicast traffic storm control, and broadcast traffic exceeds the level within the 10-millisecond interval, traffic storm control drops all broadcast and multicast traffic until the end of the interval.
- If you enable broadcast and multicast traffic storm control, and multicast traffic exceeds the level within the 10-millisecond interval, traffic storm control drops all broadcast and multicast traffic until the end of the interval.

By default, the Cisco NX-OS software takes no corrective action when the traffic exceeds the configured level. However, you can configure an Embedded Event Management (EEM) action to error-disable an interface if the traffic does not subside (drop below the threshold) within a certain time period. For information on configuring EEM, see the *Cisco Nexus 7000 Series NX-OS System Management Command Reference*.

Virtualization Support for Traffic Storm Control

Traffic storm control configuration and operation are local to the virtual device context (VDC).

For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Licensing Requirements for Traffic Storm Control

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	Traffic storm control 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 an explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Guidelines and Limitations for Traffic Storm Control

When configuring the traffic storm control level, note the following guidelines and limitations:

- Only one suppression level is shared by all three suppression modes i.e., unicast, multicast, and broadcast. For example, if you set the broadcast level to 30 and then set the multicast level to 40, both levels are enabled and set to 40.
- You can configure traffic storm control on a port-channel interface.
- Do not configure traffic storm control on interfaces that are members of a port-channel interface. Configuring traffic storm control on interfaces that are configured as members of a port channel puts the ports into a suspended state.
- When you use the **storm-control unicast level** *percentage* command in a module, both the unknown and known unicast traffic gets discarded after reaching the threshold value.
- Traffic storm control on all Cisco FEX devices connected to Cisco Nexus 7000 series switches has following guidelines and limitations:
    - Traffic storm control is not supported on HIF ports.
    - Traffic storm control is supported only on NIF ports.
- Specify the level as a percentage of the total interface bandwidth:
    - The level can be from 0 to 100.
    - The optional fraction of a level can be from 0 to 99.
    - 100 percent means no traffic storm control.
    - 0.0 percent suppresses all traffic.

Because of hardware limitations and the method by which packets of different sizes are counted, the level percentage is an approximation. Depending on the sizes of the frames that make up the incoming traffic, the actual enforced level might differ from the configured level by several percentage points.

Note 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 Traffic Storm Control

This table lists the default settings for traffic storm control parameters.

Table 45: Default Traffic Storm Control Parameters

Parameters	Default
Traffic storm control	Disabled
Threshold percentage	100

Configuring Traffic Storm Control

You can set the percentage of total available bandwidth that the controlled traffic can use.

Note Traffic storm control uses a 10-millisecond interval that can affect the behavior of traffic storm control.

SUMMARY STEPS

1. **configure terminal**
2. **interface** {**ethernet** *slot/port* | **port-channel** *number*}
3. **storm-control** {**broadcast** | **multicast** | **unicast**} **level** *percentage*[**.***fraction*]
4. **exit**
5. (Optional) **show running-config interface** {**ethernet** *slot/port* | **port-channel** *number*}
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**interface** {**ethernet** *slot*/*port* | **port-channel** *number*}
	Example:
	`switch# interface ethernet 1/1`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** *percentage*[**.***fraction*] **Example:** `switch(config-if)# storm-control unicast level 40`	Configures traffic storm control for traffic on the interface. The default state is disabled. **Note** The **storm-control unicast** command configures traffic storm control for all the unicast packets.

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 5	(Optional) **show running-config interface** {**ethernet** *slot*/*port* | **port-channel** *number*} **Example:** `switch(config)# show running-config interface ethernet 1/1`	Displays the traffic storm control 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.

Verifying Traffic Storm Control Configuration

To display traffic storm control configuration information, perform one of the following tasks:

Command	Purpose
show interface [**ethernet** *slot*/*port* | **port-channel** *number*] **counters storm-control**	Displays the traffic storm control configuration for the interfaces.
show running-config interface	Displays the traffic storm control configuration.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Monitoring Traffic Storm Control Counters

You can monitor the counters the Cisco NX-OS device maintains for traffic storm control activity.

SUMMARY STEPS

1. **show interface** [**ethernet** *slot/port* | **port-channel** *number*] **counters storm-control**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show interface** [**ethernet** *slot/port* | **port-channel** *number*] **counters storm-control** **Example:** `switch# show interface counters storm-control`	Displays the traffic storm control counters.

Configuration Example for Traffic Storm Control

The following example shows how to configure traffic storm control:

```
interface Ethernet1/1
  storm-control broadcast level 40
  storm-control multicast level 40
  storm-control unicast level 40
```

Additional References for Traffic Storm Control

This section includes additional information related to implementing traffic storm control.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

Feature History for Traffic Storm Control

This table lists the release history for this feature.

Table 46: Feature History for Traffic Storm Control

Feature Name	Releases	Feature Information
Traffic storm control	6.0(1)	No change from Release 5.2.
Traffic storm control	5.2(1)	No change from release 5.1.
Traffic storm control	5.1(1)	No change from Release 5.0.

Feature Name	Releases	Feature Information
Traffic storm control	5.0(2)	No change from Release 4.2.
Traffic storm control	4.2(1)	No change from Release 4.1.

CHAPTER 24

Configuring Unicast RPF

This chapter describes how to configure rate limits for egress traffic on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Unicast RPF

The Unicast RPF feature reduces problems that are caused by the introduction of malformed or forged (spoofed) IPv4 or IPv6 source addresses into a network by discarding IPv4 or IPv6 packets that lack a verifiable IP source address. For example, a number of common types of Denial-of-Service (DoS) attacks, including Smurf and Tribal Flood Network (TFN) attacks, can take advantage of forged or rapidly changing source IPv4 or IPv6 addresses to allow attackers to thwart efforts to locate or filter the attacks. Unicast RPF deflects attacks by forwarding only the packets that have source addresses that are valid and consistent with the IP routing table.

When you enable Unicast RPF on an interface, the device examines all ingress packets received on that interface to ensure that the source address and source interface appear in the routing table and match the interface on which the packet was received. This examination of source addresses relies on the Forwarding Information Base (FIB).

Note Unicast RPF is an ingress function and is applied only on the ingress interface of a device at the upstream end of a connection.

Unicast RPF verifies that any packet received at a device interface arrives on the best return path (return route) to the source of the packet by doing a reverse lookup in the FIB. If the packet was received from one of the best reverse path routes, the packet is forwarded as normal. If there is no reverse path route on the same interface from which the packet was received, the source address might have been modified by the attacker. If Unicast RPF does not find a reverse path for the packet, the packet is dropped.

Note With Unicast RPF, all equal-cost "best" return paths are considered valid, which means that Unicast RPF works where multiple return paths exist, if each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Interior Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

Unicast RPF Process

Unicast RPF has several key implementation principles:

- The packet must be received at an interface that has the best return path (route) to the packet source (a process called *symmetric routing*). There must be a route in the FIB that matches the route to the receiving interface. Static routes, network statements, and dynamic routing add routes to the FIB.
- IP source addresses at the receiving interface must match the routing entry for the interface.
- Unicast RPF is an input function and is applied only on the input interface of a device at the upstream end of a connection.

You can use Unicast RPF for downstream networks, even if the downstream network has other connections to the Internet.

Caution Be careful when using optional BGP attributes, such as weight and local preference, because an attacker can modify the best path back to the source address. Modification would affect the operation of Unicast RPF.

When a packet is received at the interface where you have configured Unicast RPF and ACLs, the Cisco NX-OS software performs the following actions:

SUMMARY STEPS

1. Checks the input ACLs on the inbound interface.
2. Uses Unicast RPF to verify that the packet has arrived on the best return path to the source, which it does by doing a reverse lookup in the FIB table.
3. Conducts a FIB lookup for packet forwarding.

4. Checks the output ACLs on the outbound interface.
5. Forwards the packet.

DETAILED STEPS

Step 1 Checks the input ACLs on the inbound interface.

Step 2 Uses Unicast RPF to verify that the packet has arrived on the best return path to the source, which it does by doing a reverse lookup in the FIB table.

Step 3 Conducts a FIB lookup for packet forwarding.

Step 4 Checks the output ACLs on the outbound interface.

Step 5 Forwards the packet.

Global Statistics

Each time the Cisco NX-OS device drops a packet at an interface due to a failed unicast RPF check, that information is counted globally on the device on a per-forwarding engine (FE) basis. Global statistics on dropped packets provide information about potential attacks on the network, but they do not specify which interface is the source of the attack. Per-interface statistics on packets dropped due to a failed unicast RPF check are not available.

Virtualization Support for Unicast RPF

Unicast RPF configuration and operation is local to the virtual device context (VDC). For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Guidelines and Limitations for Unicast RPF

Unicast RPF has the following configuration guidelines and limitations:

- You must apply Unicast RPF at the interface downstream from the larger portion of the network, preferably at the edges of your network.
- The further downstream that you apply Unicast RPF, the finer the granularity you have in mitigating address spoofing and in identifying the sources of spoofed addresses. For example, applying Unicast RPF on an aggregation device helps to mitigate attacks from many downstream networks or clients and is simple to administer, but it does not help identify the source of the attack. Applying Unicast RPF at the network access server helps limit the scope of the attack and trace the source of the attack; however, deploying Unicast RPF across many sites does add to the administration cost of operating the network.
- The more entities that deploy Unicast RPF across Internet, intranet, and extranet resources, means that the better the chances are of mitigating large-scale network disruptions throughout the Internet community, and the better the chances are of tracing the source of an attack.

- Unicast RPF will not inspect IP packets that are encapsulated in tunnels, such as generic routing encapsulation (GRE) tunnels. You must configure Unicast RPF at a home gateway so that Unicast RPF processes network traffic only after the tunneling and encryption layers have been stripped off the packets.
- You can use Unicast RPF in any “single-homed” environment where there is only one access point out of the network or one upstream connection. Networks that have one access point provide symmetric routing, which means that the interface where a packet enters the network is also the best return path to the source of the IP packet.
- Do not use Unicast RPF on interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, which means that multiple routes to the source of a packet exist. You should configure Unicast RPF only where there is natural or configured symmetry. Do not configure strict Unicast RPF.
- Unicast RPF allows packets with 0.0.0.0 source and 255.255.255.255 destination to pass so that the Bootstrap Protocol (BOOTP) and the Dynamic Host Configuration Protocol (DHCP) can operate correctly.

Note 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 Unicast RPF

This table lists the default settings for Unicast RPF parameters.

Table 47: Default Unicast RPF Parameter Settings

Parameters	Default
Unicast RPF	Disabled

Configuring Unicast RPF

You can configure one the following Unicast RPF modes on an ingress interface:

Strict Unicast RPF mode
A strict mode check is successful when Unicast RFP finds a match in the FIB for the packet source address and the ingress interface through which the packet is received matches one of the Unicast RPF interfaces in the FIB match. If this check fails, the packet is discarded. You can use this type of Unicast RPF check where packet flows are expected to be symmetrical.

Loose Unicast RPF mode
A loose mode check is successful when a lookup of a packet source address in the FIB returns a match and the FIB result indicates that the source is reachable through at least one real interface. The ingress interface through which the packet is received is not required to match any of the interfaces in the FIB result.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **ip verify unicast source reachable-via** {**any** [**allow-default**] | **rx**}
4. **ipv6 verify unicast source reachable-via** {**any** [**allow-default**] | **rx**}
5. **exit**
6. (Optional) **show ip interface ethernet** *slot*/*port*
7. (Optional) **show running-config interface ethernet** *slot*/*port*
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot*/*port*
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		Specifies an Ethernet interface and enters interface configuration mode.

Step 3	**ip verify unicast source reachable-via** {**any** [**allow-default**] | **rx**} **Example:** `switch(config-if)# ip verify unicast source reachable-via any`	Configures Unicast RPF on the interface for IPv4. The **any** keyword specifies loose Unicast RPF. If you specify the **allow-default** keyword, the source address lookup can match the default route and use that for verification. The **rx** keyword specifies strict Unicast RPF.
Step 4	**ipv6 verify unicast source reachable-via** {**any** [**allow-default**] | **rx**} **Example:** `switch(config-if)# ipv6 verify unicast source reachable-via any`	Configures Unicast RPF on the interface for IPv6. The **any** keyword specifies loose Unicast RPF. If you specify the **allow-default** keyword, the source address lookup can match the default route and use that for verification. The **rx** keyword specifies strict Unicast RPF.

Step 5	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 6	(Optional) **show ip interface ethernet** *slot*/*port* **Example:** `switch(config)# show ip interface ethernet 2/3`	Displays the IP information for an interface.

	Command or Action	Purpose
Step 7	(Optional) **show running-config interface ethernet** *slot/port* **Example:** `switch(config)# show running-config interface ethernet 2/3`	Displays the configuration for an interface in the running configuration.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuration Examples for Unicast RPF

The following example shows how to configure loose Unicast RFP for IPv4 packets:

```
interface Ethernet2/3
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via any
```

The following example shows how to configure strict Unicast RFP for IPv4 packets:

```
interface Ethernet2/2
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via rx
```

The following example shows how to configure loose Unicast RFP for IPv6 packets:

```
interface Ethernet2/1
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via any
```

The following example shows how to configure strict Unicast RFP for IPv6 packets:

```
interface Ethernet2/4
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via rx
```

Verifying the Unicast RPF Configuration

To display Unicast RPF configuration information, perform one of the following tasks:

Command	Purpose
show running-config interface ethernet *slot/port*	Displays the interface configuration in the running configuration.

Command	Purpose
show running-config ip [**all**]	Displays the IPv4 configuration in the running configuration.
show running-config ipv6 [**all**]	Displays the IPv6 configuration in the running configuration.
show startup-config interface ethernet *slot/port*	Displays the interface configuration in the startup configuration.
show startup-config ip	Displays the IP configuration in the startup configuration.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Additional References for Unicast RPF

This section includes additional information related to implementing Unicast RPF.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

Feature History for Unicast RPF

This table lists the release history for this feature.

Table 48: Feature History for Unicast RPF

Feature Name	Releases	Feature Information	
Unicast RPF	6.0(1)	No change from Release 5.2.	
Unicast RPF	5.2(1)	No change from Release 5.1.	
Unicast RPF	5.1(1)	No change from Release 5.0.	
Unicast RPF	5.0(2)	No change from Release 4.2.	
Unicast RPF	4.2(1)	No change from Release 4.1.	

CHAPTER 25

Configuring Control Plane Policing

This chapter contains the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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 different mechanisms to control the rate at which packets arrive at the supervisor module. Two mechanisms control the rate of traffic to the supervisor module. One is called policing and the other is called rate limiting.

Using hardware policers, you can define separate actions for traffic that conforms to, exceeds, or violates certain conditions. The 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 or a percentage of the link rate.

Peak information rate (PIR)
Desired bandwidth, specified as a bit rate or a percentage of the link rate.

Committed burst (BC)
Size of a traffic burst that can exceed the CIR within a given unit of time and not impact scheduling.
Extended burst (BE)
Size that a traffic burst can reach before all traffic exceeds the PIR.

In addition, you can set separate actions such as transmit or drop for conform, exceed, and violate traffic.

For more information on policing parameters, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide*.

Default Policing Policies

When you bring up your Cisco NX-OS device for the first time, the Cisco NX-OS software installs the default copp-system-p-policy-strict policy to protect the supervisor module from DoS attacks. You can set the level of protection by choosing one of the following CoPP policy options from the initial setup utility:

- Strict—This policy is 1 rate and 2 color and has a BC value of 250 ms (except for the important class, which has a value of 1000 ms).
- Moderate—This policy is 1 rate and 2 color and has a BC value of 310 ms (except for the important class, which has a value of 1250 ms). These values are 25 percent greater than the strict policy.
- Lenient—This policy is 1 rate and 2 color and has a BC value of 375 ms (except for the important class, which has a value of 1500 ms). These values are 50 percent greater than the strict policy.
- Dense—This policy is 1 rate and 2 color. The classes critical, normal, redirect, exception, undesirable, l2-default, and default have a BC value of 250 ms. The classes important, management, normal-dhcp, normal-dhcp-relay-response, and monitoring have a BC value of 1000 ms. The class l2-unpoliced has a BC value of 5 MB.

  Note We recommend this default policy when the chassis is fully loaded with F2 Series modules or loaded with more F2 Series modules than any other I/O modules.

- Skip—No control plane policy is applied. In Cisco NX-OS releases prior to 5.2, this option is named none.

If you do not select an option or choose not to execute the setup utility, the Cisco NX-OS software applies strict policing. We recommend that you start with the strict policy and later modify the CoPP policies as required.

The copp-system-p-policy policy has optimized values suitable for basic device operations. You must add specific class and access-control list (ACL) rules that meet your DoS protection requirements. The default CoPP policy does not change when you upgrade the Cisco NX-OS software.

Caution Selecting the **skip** option and not subsequently configuring CoPP protection can leave your Cisco NX-OS device vulnerable to DoS attacks.

You can reassign the CoPP default policy by entering the setup utility again using the **setup** command from the CLI prompt or by using the **copp profile** command in Cisco NX-OS Release 5.2 or later releases.

Related Topics

Changing or Reapplying the Default CoPP Policy, on page 648

Default Class Maps

Note The class maps provided here are for Cisco NX-OS Release 6.2(2). Some of the values might vary for previous releases.

The copp-system-class-exception class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-exception
    match exception ip option
    match exception ip icmp unreachable
    match exception ipv6 option
    match exception ipv6 icmp unreachable
```

The copp-system-class-critical class has the following configuration:

```
ip access-list copp-system-p-acl-igmp
    permit igmp any 224.0.0.0/3

ip access-list copp-system-p-acl-lisp
    permit udp any any eq 4342

ip access-list copp-system-p-acl-msdp
    permit tcp any gt 1024 any eq 639
    permit tcp any eq 639 any gt 1024

ip access-list copp-system-p-acl-bgp
    permit tcp any gt 1024 any eq bgp
    permit tcp any eq bgp any gt 1024

ip access-list copp-system-p-acl-eigrp
    permit eigrp any any

ip access-list copp-system-p-acl-lisp6
    permit udp any any eq 4342

ip access-list copp-system-p-acl-rip
    permit udp any 224.0.0.0/24 eq rip

ip access-list copp-system-p-acl-ospf
    permit ospf any any

ip access-list copp-system-p-acl-pim
    permit pim any 224.0.0.0/24


    permit udp any any eq 496
    permit ip any 224.0.0.13/32

ipv6 access-list copp-system-p-acl-bgp6
    permit tcp any gt 1024 any eq bgp
    permit tcp any eq bgp any gt 1024

ipv6 access-list copp-system-p-acl-ospf6
    permit 89 any any
```

```
ipv6 access-list copp-system-p-acl-pim6
    permit 103 any FF02::D/128
    permit udp any any eq pim-auto-rp

ipv6 access-list copp-system-p-acl-rip6
    permit udp any ff02::9/64 eq 521

ip access-list copp-system-p-acl-vpc
    permit udp any any eq 3200

ip access-list copp-system-p-acl-mpls-ldp
    permit udp any eq 646 any eq 646
    permit tcp any any eq 646
    permit tcp any eq 646 any

ip access-list copp-system-p-acl-mpls-oam
    permit udp any eq 3503 any

ip access-list copp-system-p-acl-mpls-rsvp
    permit 46 any any

ip access-list copp-system-p-acl-otv-as
    permit udp any any eq 8472

mac access-list copp-system-p-acl-mac-l2pt
  permit any 0100.0ccd.cdd0 0000.0000.0000

mac access-list copp-system-p-acl-mac-otv-isis
  permit any 0100.0cdf.dfdf 0000.0000.0000

mac access-list copp-system-p-acl-mac-fabricpath-isis
  permit any 0180.c200.0041 0000.0000.0000

mac access-list copp-system-p-acl-mac-l3-isis
    permit any 0180.c200.0015 0000.0000.0000
    permit any 0180.c200.0014.0000.0000.0000

class-map type control-plane match-any copp-system-p-class-critical
    match access-group name copp-system-p-acl-bgp
    match access-group name copp-system-p-acl-rip
    match access-group name copp-system-p-acl-vpc
    match access-group name copp-system-p-acl-bgp6
    match access-group name copp-system-p-acl-lisp
    match access-group name copp-system-p-acl-ospf
    match access-group name copp-system-p-acl-rip6
    match access-group name copp-system-p-acl-eigrp
    match access-group name copp-system-p-acl-lisp6
    match access-group name copp-system-p-acl-ospf6
    match access-group name copp-system-p-acl-eigrp6
    match access-group name copp-system-p-acl-otv-as
    match access-group name copp-system-p-acl-mac-l2pt
    match access-group name copp-system-p-acl-mpls-ldp
    match access-group name copp-system-p-acl-mpls-oam
    match access-group name copp-system-p-acl-mpls-rsvp
    match access-group name copp-system-p-acl-mac-l3-isis
    match access-group name copp-system-p-acl-mac-otv-isis
    match access-group name copp-system-p-acl-mac-fabricpath-isis
    match protocol mpls router-alert
    match protocol mpls exp 6
```

Note The LISP, LISP6, and MAC Layer 3 IS-IS ACLs were added in Cisco NX-OS Release 6.1.

The copp-system-class-important class has the following configuration:

```
ip access-list copp-system-p-acl-hsrp
    permit udp any 224.0.0.2/32 eq 1985
    permit udp any 224.0.0.102/32 eq 1985
```

Note Beginning with Cisco NX-OS Release 6.2(2), the HSRP control packets use predefined destination addresses, as shown above. In Cisco NX-OS releases prior to 6.2(2), the Hot Standby Router Protocol (HSRP) ACL has a lenient entry, with the last octet ignored, as shown in the following configuration:

```
ip access-list copp-system-p-acl-hsrp
    permit udp any 224.0.0.0/24 eq 1985
```

```
ipv6 access-list copp-system-p-acl-hsrp6
    permit udp any ff02::66/128 eq 2029

ip access-list copp-system-p-acl-vrrp

    permit ip any 224.0.0.18/32

ip access-list copp-system-p-acl-glbp
    permit udp any eq 3222 224.0.0.0/24 eq 3222

ip access-list copp-system-p-acl-pim-reg
    permit pim any any

ipv6 access-list copp-system-p-acl-icmp6-msgs
    permit icmp any any router-advertisement
    permit icmp any any router-solicitation
    permit icmp any any nd-na
    permit icmp any any nd-ns
    permit icmp any any mld-query
    permit icmp any any mld-report
    permit icmp any any mld-reduction
    permit icmp any any 143

ip access-list copp-system-p-acl-cts
    permit tcp any any eq 64999
    permit tcp any eq 64999 any

ip access-list copp-system-p-acl-pim-mdt-join
    permit udp any 224.0.0.13/32

ipv6 access-list copp-system-p-acl-vrrp6
    permit ipv6 any ff02::12/128

ip access-list copp-system-p-acl-wccp

    permit udp any eq 2048 any eq 2048

mac access-list copp-system-p-acl-mac-lldp
  permit any 0180.c200.000c 0000.0000.0000 0x88cc

mac access-list copp-system-p-acl-mac-flow-control
  permit any 0180.c200.0001 0000.0000.0000 0x8808
```

```
class-map type control-plane match-any copp-system-p-class-important
    match access-group name copp-system-p-acl-cts
    match access-group name copp-system-p-acl-glbp
    match access-group name copp-system-p-acl-hsrp
    match access-group name copp-system-p-acl-vrrp
    match access-group name copp-system-p-acl-wccp
    match access-group name copp-system-p-acl-hsrp6
    match access-group name copp-system-p-acl-vrrp6
    match access-group name copp-system-p-acl-mac-lldp
    match access-group name copp-system-p-acl-mac-flow-control
```

Note The "permit icmp any any 143" rule was added to the acl-icmp6-msgs ACL to support the MLDv2 report in Cisco NX-OS Release 6.1.

Note The VRRP6 ACL was added in Cisco NX-OS Release 6.2(2).

Note Beginning with Cisco NX-OS Release 6.2(2), the behavior of multicast traffic has changed from being policed at different rates in different classes to being grouped into three classes (multicast-host, multicast-router, and normal) and policed at consistent rates, depending on the type of multicast traffic, as follows:

```
ip access-list copp-system-p-acl-igmp
  permit igmp any 224.0.0.0/3
ipv6 access-list copp-system-p-acl-mld
  permit icmp any any mld-query
  permit icmp any any mld-report
  permit icmp any any mld-reduction
  permit icmp any any 143
ip access-list copp-system-p-acl-msdp
  permit tcp any gt 1024 any eq 639
  permit tcp any eq 639 any gt 1024
ipv6 access-list copp-system-p-acl-ndp
  permit icmp any any router-solicitation
  permit icmp any any router-advertisement
  permit icmp any any 137
  permit icmp any any nd-ns
  permit icmp any any nd-na
ip access-list copp-system-p-acl-pim
  permit pim any 224.0.0.0/24
  permit udp any any eq 496
  permit ip any 224.0.0.13/32
ip access-list copp-system-p-acl-pim-mdt-join
  permit udp any 224.0.0.13/32
ip access-list copp-system-p-acl-pim-reg
  permit pim any any
ipv6 access-list copp-system-p-acl-pim6
  permit pim any ff02::d/128
  permit udp any any eq 496
ipv6 access-list copp-system-p-acl-pim6-reg
  permit pim any any
mac access-list copp-system-p-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e
class-map type control-plane match-any copp-system-p-class-multicast-host
  match access-group name copp-system-p-acl-mld
```

```
  match access-group name copp-system-p-acl-igmp
class-map type control-plane match-any copp-system-p-class-multicast-router
  match access-group name copp-system-p-acl-pim
  match access-group name copp-system-p-acl-msdp
  match access-group name copp-system-p-acl-pim6
  match access-group name copp-system-p-acl-pim-reg
  match access-group name copp-system-p-acl-pim6-reg
  match access-group name copp-system-p-acl-pim-mdt-join
class-map type control-plane match-any copp-system-p-class-ndp
  match access-group name copp-system-p-acl-ndp
```

The copp-system-class-management class has the following configuration:

```
ip access-list copp-system-p-acl-tacacs
    permit tcp any any eq tacacs
    permit tcp any eq tacacs any

ip access-list copp-system-p-acl-radius
    permit udp any any eq 1812
    permit udp any any eq 1813
    permit udp any any eq 1645
    permit udp any any eq 1646
    permit udp any eq 1812 any
    permit udp any eq 1813 any
    permit udp any eq 1645 any
    permit udp any eq 1646 any

ip access-list copp-system-p-acl-ntp
    permit udp any any eq ntp

ip access-list copp-system-p-acl-ftp
    permit tcp any any eq ftp-data
    permit tcp any any eq ftp
    permit tcp any eq ftp-data any
    permit tcp any eq ftp any

ip access-list copp-system-p-acl-tftp
    permit udp any any eq tftp
    permit udp any any eq 1758
    permit udp any eq tftp any
    permit udp any eq 1758 any

ip access-list copp-system-p-acl-sftp
    permit tcp any any eq 115
    permit tcp any eq 115 any

ip access-list copp-system-p-acl-ssh
    permit tcp any any eq 22
    permit tcp any eq 22 any

ip access-list copp-system-p-acl-snmp
    permit udp any any eq snmp
    permit udp any any eq snmptrap

ip access-list copp-system-p-acl-telnet
    permit tcp any any eq telnet
    permit tcp any any eq 107
    permit tcp any eq telnet any
    permit tcp any eq 107 any

ipv6 access-list copp-system-p-acl-tacacs6
    permit tcp any any eq tacacs
    permit tcp any eq tacacs any
```

```
ipv6 access-list copp-system-p-acl-radius6
    permit udp any any eq 1812
    permit udp any any eq 1813
    permit udp any any eq 1645
    permit udp any any eq 1646
    permit udp any eq 1812 any
    permit udp any eq 1813 any
    permit udp any eq 1645 any
    permit udp any eq 1646 any

ipv6 access-list copp-system-p-acl-ntp6
    permit udp any any eq ntp
    permit udp any eq ntp any

ipv6 access-list copp-system-p-acl-tftp6
    permit udp any any eq tftp
    permit udp any any eq 1758
    permit udp any eq tftp any
    permit udp any eq 1758 any

ipv6 access-list copp-system-p-acl-ssh6
    permit tcp any any eq 22
    permit tcp any eq 22 any

ipv6 access-list copp-system-p-acl-telnet6
    permit tcp any any eq telnet
    permit tcp any any eq 107
    permit tcp any eq telnet any
    permit tcp any eq 107 any

class-map type control-plane match-any copp-system-p-class-management
    match access-group name copp-system-p-acl-tacacs
    match access-group name copp-system-p-acl-radius
    match access-group name copp-system-p-acl-ntp
    match access-group name copp-system-p-acl-ftp
    match access-group name copp-system-p-acl-tftp
    match access-group name copp-system-p-acl-sftp
    match access-group name copp-system-p-acl-ssh
    match access-group name copp-system-p-acl-snmp
    match access-group name copp-system-p-acl-telnet
    match access-group name copp-system-p-acl-tacacs6
    match access-group name copp-system-p-acl-radius6
    match access-group name copp-system-p-acl-ntp6
    match access-group name copp-system-p-acl-tftp6
    match access-group name copp-system-p-acl-ssh6
    match access-group name copp-system-p-acl-telnet6
```

The copp-system-class-normal class has the following configuration:

```
ip access-list copp-system-p-acl-dhcp
  permit udp any neq bootps any eq bootps
  permit udp any eq bootpc any

ip access-list copp-system-p-acl-dhcp-relay-response
  permit udp any eq bootps any
  permit udp any any eq bootpc

mac access-list copp-system-p-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e

class-map type control-plane match-any copp-system-p-class-normal
   match access-group name copp-system-p-acl-mac-dot1x
   match exception multicast directly-connected-sources
```

```
   match protocol arp

class-map type control-plane match-any copp-system-p-class-normal-dhcp
  match redirect dhcp-snoop
  match access-group name copp-system-p-acl-dhcp

class-map type control-plane match-any copp-system-p-class-normal-dhcp-relay-response
  match access-group name copp-system-p-acl-dhcp-relay-response
```

The copp-system-class-redirect class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-redirect
    match redirect arp-inspect
```

The copp-system-class-monitoring class has the following configuration:

```
ip access-list copp-system-p-acl-icmp
    permit icmp any any echo
    permit icmp any any echo-reply

ip access-list copp-system-p-acl-traceroute
    permit icmp any any ttl-exceeded
    permit icmp any any port-unreachable
    permit udp any any range 33434 33534

ipv6 access-list copp-system-p-acl-icmp6
    permit icmp any any echo-request
    permit icmp any any echo-reply

class-map type control-plane match-any copp-system-p-class-monitoring
    match access-group name copp-system-p-acl-icmp
    match access-group name copp-system-p-acl-traceroute
    match access-group name copp-system-p-acl-icmp6
```

The copp-system-class-l2-unpoliced class has the following configuration:

```
mac access-list copp-system-p-acl-mac-cdp-udld-vtp
    permit any 0100.0ccc.cccc 0000.0000.0000

mac access-list copp-system-p-acl-mac-stp
    permit any 0100.0ccc.cccd 0000.0000.0000
    permit any 0180.c200.0000 0000.0000.0000

mac access-list copp-system-p-acl-mac-lacp
    permit any 0180.c200.0002 0000.0000.0000 0x8809

mac access-list copp-system-p-acl-mac-cfsoe
    permit any 0180.C200.000E 0000.0000.0000 0x8843

mac access-list copp-system-p-acl-mac-l2-tunnel
    permit any any 0x8840

class-map type control-plane copp-system-p-class-l2-unpoliced
    match access-group name copp-system-p-acl-mac-stp
    match access-group name copp-system-p-acl-mac-lacp
    match access-group name copp-system-p-acl-mac-cfsoe
    match access-group name copp-system-p-acl-mac-sdp-srp
    match access-group name copp-system-p-acl-mac-l2-tunnel
```

Note The MAC Layer 2 tunnel ACL was added in Cisco NX-OS Release 6.1.

The copp-system-class-l2-default class has the following configuration:

```
mac access-list copp-system-p-acl-mac-undesirable
    permit any any

class-map type control-plane copp-system-p-class-l2-default
    match access-group name copp-system-p-acl-mac-undesirable
    match protocol mpls
```

The copp-system-class-fcoe class has the following configuration:

```
mac access-list copp-system-p-acl-mac-fcoe
    permit any any 0x8906
    permit any any 0x8914

class-map type control-plane match-any copp-system-p-class-fcoe
    match access-group name copp-system-p-acl-mac-fcoe
```

Note The copp-system-class-fcoe class was added in Cisco NX-OS Release 6.1.

The copp-system-class-undesirable class has the following configuration:

```
ip access-list copp-system-p-acl-undesirable
    permit udp any any eq 1434

class-map type control-plane match-any copp-system-p-class-undesirable
    match access-group name copp-system-p-acl-undesirable
    match exception fcoe-fib-miss
```

Note The fcoe-fib-miss match exception was added in Cisco NX-OS Release 6.1.

```
mac access-list copp-system-acl-mac-cdp-udld-vtp
  permit any 0100.0ccc.cccc 0000.0000.0000
mac access-list copp-system-acl-mac-cfsoe
  permit any 0180.c200.000e 0000.0000.0000 0x8843
mac access-list copp-system-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e
mac access-list copp-system-acl-mac-flow-control
  permit any 0180.c200.0001 0000.0000.0000 0x8808
mac access-list copp-system-acl-mac-l2mp-isis
  permit any 0180.c200.0015 0000.0000.0000
  permit any 0180.c200.0014 0000.0000.0000
mac access-list copp-system-acl-mac-l2pt
  permit any 0100.0ccd.cdd0 0000.0000.0000
mac access-list copp-system-acl-mac-lacp
  permit any 0180.c200.0002 0000.0000.0000 0x8809
```

```
mac access-list copp-system-acl-mac-lldp
  permit any 0180.c200.000e 0000.0000.0000 0x88c
mac access-list copp-system-acl-mac-stp
  permit any 0100.0ccc.cccd 0000.0000.0000
  permit any 0180.c200.0000 0000.0000.0000
mac access-list copp-system-acl-mac-undesirable
  permit any any
```

Strict Default CoPP Policy

The strict CoPP policy has the following configuration:

```
policy-map type control-plane copp-system-p-policy-strict

    class copp-system-p-class-critical
        set cos 7
        police cir 36000 kbps bc 250 ms conform transmit violate drop

    class copp-system-p-class-important
        set cos 6
        police cir 1400 kbps bc 1500 ms conform transmit violate drop

    class copp-system-p-class-multicast-router
        set cos 6
        police cir 2600 kbps bc 1000 ms conform transmit violate drop

    class copp-system-p-class-management
        set cos 2
        police cir 10000 kbps bc 250 ms conform transmit violate drop

    class copp-system-p-class-multicast-host
        set cos 1
        police cir 1000 kbps bc 1000 ms conform transmit violate drop

    class copp-system-p-class-normal
        set cos 1
        police cir 680 kbps bc 250 ms conform transmit violate drop

    class copp-system-p-class-ndp
        set cos 6
        police cir 680 kbps bc 250 ms conform transmit violate drop

    class copp-system-p-class-normal-dhcp
        set cos 1
        police cir 1500 kbps bc 250 ms conform transmit violate drop

    class copp-system-p-class-normal-dhcp-relay-response
        set cos 1
        police cir 1800 kbps bc 500 ms conform transmit violate drop

    class copp-system-p-class-redirect
        set cos 1
        police cir 280 kbps bc 250 ms conform transmit violate drop

    class copp-system-p-class-exception
        set cos 1
        police cir 360 kbps bc 250 ms conform transmit violate drop

    class copp-system-p-class-monitoring
        set cos 1
        police cir 130 kbps bc 1000 ms conform transmit violate drop
```

```
    class copp-system-p-class-l2-unpoliced
        police cir 8 gbps bc 5 mbytes conform transmit violate transmit

    class copp-system-p-class-undesirable
        set cos 0
        police cir 32 kbps bc 250 ms conform drop violate drop

    class copp-system-p-class-fcoe
        set cos 6
        police cir 1060 kbps bc 1000 ms conform transmit violate drop

    class copp-system-p-class-l2-default
        police cir 10 kbps bc 250 ms conform transmit violate drop

    class class-default
        set cos 0
        police cir 10 kbps bc 250 ms conform transmit violate drop
```

Note The copp-system-p-class-fcoe class was added in Cisco NX-OS Release 6.1. The copp-system-p-class-multicast-router and copp-system-p-class-multicast-host classes were added in Cisco NX-OS Release 6.2(2).

Moderate Default CoPP Policy

The moderate CoPP policy has the following configuration:

```
policy-map type control-plane copp-system-p-policy-moderate

    class copp-system-p-class-critical
        set cos 7
        police cir 36000 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-important
        set cos 6
        police cir 1400 kbps bc 1250 ms conform transmit violate drop

    class copp-system-p-class-multicast-router
        set cos 6
        police cir 2600 kbps bc 1000 ms conform transmit violate drop

    class copp-system-p-class-management
        set cos 2
        police cir 10000 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-multicast-host
        set cos 1
        police cir 1000 kbps bc 1000 ms conform transmit violate drop

    class copp-system-p-class-normal
        set cos 1
        police cir 680 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-ndp
        set cos 6
        police cir 680 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-normal-dhcp
        set cos 1
```

```
        police cir 1500 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-normal-dhcp-relay-response
        set cos 1
        police cir 1800 kbps bc  620  ms conform transmit violate drop

    class copp-system-p-class-redirect
        set cos 1
        police cir 280 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-exception
        set cos 1
        police cir 360 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-monitoring
        set cos 1
        police cir 130 kbps bc 1250 ms conform transmit violate drop

    class copp-system-p-class-l2-unpoliced
        police cir 8 gbps bc 5 mbytes conform transmit violate transmit

    class copp-system-p-class-undesirable
        set cos 0
        police cir 32 kbps bc 310 ms conform drop violate drop

    class copp-system-p-class-fcoe
        set cos 6
        police cir 1060 kbps bc 1250 ms conform transmit violate drop

    class copp-system-p-class-l2-default
        police cir 10 kbps bc 310 ms conform transmit violate drop

    class class-default
        set cos 0
        police cir 10 kbps bc 250 ms conform transmit violate drop
```

Note The copp-system-p-class-fcoe class was added in Cisco NX-OS Release 6.1. The copp-system-p-class-multicast-router and copp-system-p-class-multicast-host classes were added in Cisco NX-OS Release 6.2(2).

Lenient Default CoPP Policy

The lenient CoPP policy has the following configuration:

```
policy-map type control-plane copp-system-p-policy-lenient

    class copp-system-p-class-critical
        set cos 7
        police cir 36000 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-important
        set cos 6
        police cir 1400 kbps bc 1500 ms conform transmit violate drop

    class copp-system-p-class-multicast-router
        set cos 6
        police cir 2600 kbps bc 1000 ms conform transmit violate drop
```

```
class copp-system-p-class-management
    set cos 2
    police cir 10000 kbps bc 375 ms conform transmit violate drop

class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 1000 ms conform transmit violate drop

class copp-system-p-class-normal
    set cos 1
    police cir 680 kbps bc 375 ms conform transmit violate drop

class copp-system-p-class-ndp
    set cos 6
    police cir 680 kbps bc 375 ms conform transmit violate drop

class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 1500 kbps bc 375 ms conform transmit violate drop

class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 1800 kbps bc 750 ms conform transmit violate drop

class copp-system-p-class-redirect
    set cos 1
    police cir 280 kbps bc 375 ms conform transmit violate drop

class copp-system-p-class-exception
    set cos 1
    police cir 360 kbps bc 375 ms conform transmit violate drop

class copp-system-p-class-monitoring
    set cos 1
    police cir 130 kbps bc 1500 ms conform transmit violate drop

class copp-system-p-class-l2-unpoliced
    police cir 8 gbps bc 5 mbytes conform transmit violate transmit

class copp-system-p-class-undesirable
    set cos 0
    police cir 32 kbps bc 375 ms conform drop violate drop

class copp-system-p-class-fcoe
    set cos 6
    police cir 1060 kbps bc 1500 ms conform transmit violate drop

class copp-system-p-class-l2-default
    police cir 10 kbps bc 375 ms conform transmit violate drop

class class-default
    set cos 0
    police cir 10 kbps bc 250 ms conform transmit violate drop
```

Note The copp-system-p-class-fcoe class was added in Cisco NX-OS Release 6.1. The copp-system-p-class-multicast-router and copp-system-p-class-multicast-host classes were added in Cisco NX-OS Release 6.2(2).

Dense Default CoPP Policy

The dense CoPP policy has the following configuration in Cisco NX-OS Release 6.2(2):

```
policy-map type control-plane copp-system-p-policy-dense
  class copp-system-p-class-critical
    set cos 7
    police cir 4500 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 1400 kbps bc 1500 ms conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 370 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 2500 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 190 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 300 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 300 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 660 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 800 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 200 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 200 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 130 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    police cir 8 gbps bc 5 mbytes conform transmit violate transmit
  class copp-system-p-class-undesirable
    set cos 0
    police cir 32 kbps bc 250 ms conform drop violate drop
  class copp-system-p-class-fcoe
    set cos 6
    police cir 600 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-l2-default
    police cir 10 kbps bc 250 ms conform transmit violate drop
  class class-default
    set cos 0
    police cir 10 kbps bc 250 ms conform transmit violate drop
```

Note The copp-system-p-class-fcoe class was added in Cisco NX-OS Release 6.1. The copp-system-p-class-multicast-router and copp-system-p-class-multicast-host classes were added in Cisco NX-OS Release 6.2(2).

Packets Per Second Credit Limit

The aggregate packets per second (PPS) for a given policy (sum of PPS of each class part of the policy) is capped by an upper PPS Credit Limit (PCL). If an increase in PPS of a given class causes a PCL exceed, the configuration is rejected. To increase the desired PPS, the additional PPS beyond PCL should be decreased from other class(es).

Modular QoS Command-Line Interface

CoPP uses the Modular Quality of Service Command-Line Interface (MQC). MQC is a CLI structure that allows you to define a traffic class, create a traffic policy (policy map), and attach the traffic policy to an interface. The traffic policy contains the CoPP feature that will be applied to the traffic class.

SUMMARY STEPS

1. Define a traffic class using the **class-map** command. A traffic class is used to classify traffic.
2. Create a traffic policy using the **policy-map** command. A traffic policy (policy map) contains a traffic class and one or more CoPP features that will be applied to the traffic class. The CoPP features in the traffic policy determine how to treat the classified traffic.
3. Attach the traffic policy (policy map) to the control plane using the **control-plane** and **service-policy** commands.

DETAILED STEPS

Step 1 Define a traffic class using the **class-map** command. A traffic class is used to classify traffic.

This example shows how to create a new class-map called copp-sample-class:

```
class-map type control-plane copp-sample-class
```

Step 2 Create a traffic policy using the **policy-map** command. A traffic policy (policy map) contains a traffic class and one or more CoPP features that will be applied to the traffic class. The CoPP features in the traffic policy determine how to treat the classified traffic.

Step 3 Attach the traffic policy (policy map) to the control plane using the **control-plane** and **service-policy** commands.

This example shows how to attach the policy map to the control plane:

```
control-plane
service-policy input copp-system-policy
```

Note The copp-system-policy is always configured and applied. There is no need to use this command explicitly.

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.

Related Topics

Configuring IP ACLs, on page 405
Configuring MAC ACLs, on page 461

Virtualization Support for CoPP

You can configure CoPP in the default virtual device context (VDC) or the admin VDC, but the CoPP configuration applies to all VDCs on the Cisco NX-OS device. For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Guidelines and Limitations for CoPP

CoPP has the following configuration guidelines and limitations:

- Support for uRPF exception CoPP class is introduced in Cisco NX-OS Release 8.2(6). By default all uRPF exception packets are punted to the supervisor module. A new CoPP class, **copp-system-p-classurpf- exception** is introduced to match uRPF exception packets and police them at 100 kbps. You can customize the default CoPP profiles and you can choose to drop uRPF exceptions or police at a lower rate.
- CoPP classification does not work for the Layer 2 control traffic in native VLAN in the following scenarios:
  - When the **native vlan** (ID other than 1) command is configured on the interface and the native VLAN ID is missing in the configuration.
  - If the **vlan dot1q tag native exclude control command** is configured.
- We recommend that you use the strict default CoPP policy initially and then later modify the CoPP policies based on the data center and application requirements.
- We recommend applying the default dense policy when the chassis is fully loaded with F2 or F2e Series modules or loaded with more F2 or F2e Series modules than any other type of I/O module.
- We recommend configuring the scale factor and applying the default dense policy when the chassis is loaded with both F2 or F2e and M Series modules.
- 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.
- We recommend 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 modify the CoPP policies.
- All the traffic that you do not specify in the other class maps is put into the last class, the default class. Monitor the drops in this class and investigate if these drops are based on traffic that you do not want or the result of a feature that was not configured and you need to add.
- All broadcast traffic is sent through CoPP logic in order to determine which packets (for example, ARP and DHCP) need to be redirected through an access control list (ACL) to the router processor. Broadcast traffic that does not need to be redirected is matched against the CoPP logic, and both conforming and

violated packets are counted in the hardware but not sent to the CPU. Broadcast traffic that needs to be sent to the CPU and broadcast traffic that does not need to be sent to the CPU must be separated into different classes.

- When you configure a policer in a CoPP class map active policy with a valid CIR value, but both conform and violate action is set to drop the packets, the CIR value will be taken as 0. The configuration of **conform drop violate drop** action drops all the classified packets irrespective of the incoming rate.

  Thus, as expected all packets will be dropped and the CoPP statistics will display the conformed counter as "0 bytes" and will not be incremented. This is an expected behaviour.

- In a CoPP policy-map, make sure you set the class with police rate as bps (bytes per second) and not as pps (packets per second). The Control plane policy segregates different packets destined for the control plane into different classes. Using hardware policers, you can define separate actions for traffic that conforms to, exceeds, or violates certain conditions. The actions can transmit the packet, mark down the packet, or drop the packet.

  The **police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} command allows you to configure the policer CIR unit in bps. But the Cisco Nexus 7000 hardware considers the byte-policing rather than the packet-policing. Therefore, you are suggested to use bps and not pps when you set the class with the police rate.

- If you remove the **set cos** configuration, there is a difference in behavior between M1 Series modules and F2/F2e Series modules with SVI and trunk ports. With an M1 Series module, when Layer 3 control packets with both DSCP and UserPriority (UP) (in the VLAN header) are received, queuing is performed using DSCP. With a F2/F2e Series module, queuing is performed using UP.

- In Cisco NX-OS releases prior to 5.2, you must use the setup utility to change or reapply the default copp-system-policy policy. You can access the setup utility using the **setup** command in the CLI.

- After you have configured CoPP, delete anything that is not being used, such as old class maps and unused routing protocols.

- You must ensure that the CoPP policy does not filter critical traffic such as routing protocols or interactive access to the device. Filtering this traffic could prevent remote access to the Cisco NX-OS device and require a console connection.

- 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).

- You can use the access control entry (ACE) hit counters in the hardware only for ACL logic. Use the software ACE hit counters and the **show access-lists** and **show policy-map type control-plane** commands to evaluate CPU traffic.

- The Cisco NX-OS device hardware performs CoPP on a per-forwarding-engine basis. CoPP does not support distributed policing. Therefore, you should choose rates so that the aggregate traffic does not overwhelm the supervisor module.

- To get a more granular view of traffic that reaches the supervisor and might be dropped by CoPP, you can use the NetFlow feature on SVIs. To do so, compare the ACL hit counts by the values listed in the NetFlow table.

- F1 Series modules do not support CoPP.

- In Cisco NX-OS Release 5.0, CoPP does not support non-IP traffic classification. Instead, you can use ACLs to drop or limit the non-IP traffic that reaches the supervisor module.

- The following rules apply beginning with Cisco NX-OS Release 5.1: The following rules apply for Cisco NX-OS Release 4.2(6):
    - CoPP supports non-IP and IP traffic classes.
    - L2PT, OTV-ISIS, and FabricPath-ISIS packets are classified under the copp-system-class-critical policy.
    - LLDP and flow-control packets are classified under the copp-system-class-important policy.
    - Dot1x packets are classified under the copp-system-class-normal policy.
    - STP, CDP, UDLD, VTP, LACP, and CFSoE packets are classified under the copp-system-class-l2-unpoliced policy. These packets are only classified; they are not policed. The corresponding policer simply displays the statistics. These packets are always forwarded to the supervisor.
    - The rest of the non-IP traffic is classified under the copp-system-class-l2-default policy.
    - IP traffic not matching any of the copp classes is classified under the class-default policy.
- CoPP MAC policies are supported beginning with Cisco NX-OS Release 5.1.
- If you use the in-service software grade (ISSU) to upgrade to Cisco NX-OS Release 5.1, the default CoPP policies for the following features must be manually configured: FabricPath, OTV, L2PT, LLDP, DHCP, and DOT1X.
- Beginning with Cisco NX-OS Release 5.2, the CoPP best practice policy is read-only. If you want to modify its configuration, you must copy it. Copied policies are treated as user configurations.
- When you use ISSU to upgrade to Cisco NX-OS Release 5.2, the policy attached to the control plane is treated as a user-configured policy. Check the CoPP profile using the **show copp profile** command and make any required changes.
- If you use the in-service software downgrade (ISSD) to downgrade from Cisco NX-OS Release 5.2, CoPP reports the incompatible configuration and instructs you to copy the CoPP profile. In the lower version, all configurations are restored in user-configuration mode.
- If you downgrade from Cisco NX-OS Release 5.2 without using ISSD, the CoPP configuration is lost, and a CoPP policy is no longer attached to the control plane.
- When you use ISSU to upgrade to a new Cisco NX-OS release, the default CoPP policy for the new release is not applied. Because you might have your own configured CoPP policy and want to continue using it, the policy for the prior release continues to be applied. However, if you have not modified the default CoPP policy in prior versions, we recommend that when you install Cisco NX-OS Release 5.2 or later releases, you apply the latest default CoPP policy for that version by using the **copp profile** [**strict** | **moderate** | **lenient**] command. This action removes the previous policy and applies the new one.
- Beginning with Cisco NX-OS Release 5.2, the default CoPP policies are read only. To make modifications, copy the default profile by using the **copp copy profile** {**strict** | **moderate** | **lenient**} {**prefix** | **suffix**} *string*, make modifications, and then apply that policy to the control plane using the **service-policy input** *policy-map-name* command.
- If multiple flows map to the same class, individual flow statistics will not be available.
- Support for monitoring CoPP with SNMP is limited to the listed cbQoSMIB tables and the elements attached to the control plane.

Note 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 49: Default CoPP Parameters Settings

Parameters	Default
Default policy	Strict
Default policy	9 policy entries **Note** The maximum number of supported policies with associated class maps is 128.
Scale factor value	1.00

Configuring CoPP

This section describes how to configure CoPP.

Configuring a Control Plane Class Map

You must configure control plane class maps for control plane policies.

You can classify traffic by matching packets based on existing ACLs. The permit and deny ACL keywords are ignored in the matching.

You can configure policies for IP version 4 (IPv4) and IP version 6 (IPv6) packets.

Before you begin

Ensure that you are in the default VDC.

Ensure that you have configured the IP ACLs if you want to use ACE hit counters in the class maps.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **class-map type control-plane** [**match-all** | **match-any**] *class-map-name*
3. (Optional) switch(config-cmap)# **match access-group name** *access-list-name*
4. (Optional) switch(config-cmap)# **match exception** {**ip** | **ipv6**} **icmp redirect**
5. (Optional) switch(config-cmap)# **match exception** {**ip** | **ipv6**} **icmp unreachable**

6. (Optional) switch(config-cmap)# **match exception** {**ip** | **ipv6**} **option**
7. (Optional) switch(config-cmap)# **match exception** {**ip** | **ipv6**} **unicast rpf-failure**
8. switch(config-cmap)# **match protocol arp**
9. (Optional) switch(config-cmap)# **match redirect arp-inspect**
10. (Optional) switch(config-cmap)# **match redirect dhcp-snoop**
11. switch(config-cmap)# **exit**
12. (Optional) switch(config)# **show class-map type control-plane** [*class-map-name*]
13. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map type control-plane** [**match-all** | **match-any**] *class-map-name*	Specifies a control plane class map and enters class map configuration mode. The default class matching is match-any. The name can be a maximum of 64 characters long and is case sensitive. **Note** You cannot use class-default, match-all, or match-any as class map names.
Step 3	(Optional) switch(config-cmap)# **match access-group name** *access-list-name*	Specifies matching for an IP ACL. **Note** The permit and deny ACL keywords are ignored in the CoPP matching.
Step 4	(Optional) switch(config-cmap)# **match exception** {**ip** | **ipv6**} **icmp redirect**	Specifies matching for IPv4 or IPv6 ICMP redirect exception packets.
Step 5	(Optional) switch(config-cmap)# **match exception** {**ip** | **ipv6**} **icmp unreachable**	Specifies matching for IPv4 or IPv6 ICMP unreachable exception packets.
Step 6	(Optional) switch(config-cmap)# **match exception** {**ip** | **ipv6**} **option**	Specifies matching for IPv4 or IPv6 option exception packets.
Step 7	(Optional) switch(config-cmap)# **match exception** {**ip** | **ipv6**} **unicast rpf-failure**	Specifies matching for IPv4 or IPv6 Unicast Reverse Path Forwarding (Unicast RPF) exception packets. For any CoPP class map, you can rate limit the IPv4 or IPv6 URPF exception packets as per the class map's rate limit configuration.
Step 8	switch(config-cmap)# **match protocol arp**	Specifies matching for IP Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP) packets.
Step 9	(Optional) switch(config-cmap)# **match redirect arp-inspect**	Specifies matching for ARP inspection redirected packets.
Step 10	(Optional) switch(config-cmap)# **match redirect dhcp-snoop**	Specifies matching for Dynamic Host Configuration Protocol (DHCP) snooping redirected packets.

	Command or Action	Purpose
Step 11	switch(config-cmap)# **exit**	Exits class map configuration mode.
Step 12	(Optional) switch(config)# **show class-map type control-plane** [*class-map-name*]	Displays the control plane class map configuration.
Step 13	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Configuring a Control Plane Policy Map

You must configure a policy map for CoPP, which includes policing parameters. If you do not configure a policer for a class, the default policer conform action is drop. The Cisco NX-OS software supports 1-rate 2-color and 2-rate 3-color policing.

The **policy-map** command is used to associate a traffic class, defined by the **class-map** command, with one or more QoS policies. The result of this association is called a service policy. A service policy contains three elements: a name, a traffic class (specified with the **class** command), and the QoS policies. The purpose of the service policy is to associate a traffic class with one or more QoS policies. Classes included within policy maps are processed top-down. When a packet is found to match a class, no further processing is performed. That is, a packet can only belong to a single class, and it is the first one to which a match occurs. When a packet does not match any of the defined classes, it is automatically placed in the class **class-default**. The default class is always applied, whether it is explicitly configured or not.

Before you begin

Ensure that you are in the default VDC.

Ensure that you have configured a control plane class map.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map type control-plane** *policy-map-name*
3. **class** {*class-map-name* [**insert-before** *class-map-name2*] | **class-default**}
4. **police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]}
5. **police** [**cir**] {cir-rate [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]
6. **police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} **conform** {**drop** | **set-cos-transmit** *cos-value* | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}]
7. **police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} **pir** *pir-rate* [**bps** | **gbps** | **kbps** | **mbps**] [[**be**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]]
8. (Optional) **logging drop threshold** [*drop-count* [**level** *syslog-level*]]
9. (Optional) **set cos** [**inner**] *cos-value*
10. (Optional) **set dscp** [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default**}
11. (Optional) **set precedence** [**tunnel**] {*prec-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**}

12. **exit**
13. **exit**
14. (Optional) **show policy-map type control-plane** [**expand**] [**name** *class-map-name*]
15. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**policy-map type control-plane** *policy-map-name*
	Example:
	`switch(config)# policy-map type control-plane ClassMapA`
	`switch(config-pmap)#`
		Specifies a control plane policy map and enters policy map configuration mode. The policy map name can have a maximum of 64 characters and is case sensitive.

Step 3	**class** {*class-map-name* [**insert-before** *class-map-name2*] | **class-default**}
	Example:
	`switch(config-pmap)# class ClassMapA`
	`switch(config-pmap-c)#`
		Specifies a control plane class map name or the class default and enters control plane class configuration mode.
		The class-default class map is always at the end of the class map list for a policy map.

Step 4	**police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} **Example:** `switch(config-pmap-c)# police cir 52000`	Specifies the committed information rate (CIR). The rate range is from 0 to 80000000000. The default CIR unit is bps.
Step 5	**police** [**cir**] {cir-rate [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**] **Example:** `switch(config-pmap-c)# police cir 52000 bc 1000`	Specifies the CIR with the committed burst (BC). The CIR range is from 0 to 80000000000 and the BC range is from 0 to 512000000. The default CIR unit is bps and the default BC size unit is **bytes**.
Step 6	**police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} **conform** {**drop** | **set-cos-transmit** *cos-value* | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}] **Example:** `switch(config-pmap-c)# police cir 52000 conform transmit exceed drop`	Specifies the CIR with the conform action. The CIR range is from 0 to 80000000000. The default rate unit is bps. The range for the *cos-value* and *prec-value* arguments is from 0 to 7. The range for the *dscp-value* argument is from 0 to 63. The options are as follows: • **drop**—Drops the packet. • **set-cos-transmit**—Sets the class of service (CoS) value. • **set-dscp-transmit**—Sets the differentiated services code point value.

	Command or Action	Purpose
		• **set-prec-transmit**—Sets the precedence value. • **transmit**—Transmits the packet. • **set dscp dscp table cir-markdown-map**—Sets the exceed action to the CIR markdown map. • **set dscp dscp table pir-markdown-map**—Sets the violate action to the PIR markdown map. **Note** You can specify the BC and conform action for the same CIR.
Step 7	**police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} **pir** *pir-rate* [**bps** | **gbps** | **kbps** | **mbps**] [[**be**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]] **Example:** `switch(config-pmap-c)# police cir 52000 pir 78000 be 2000`	Specifies the CIR with the peak information rate (PIR). The CIR range is from 0 to 80000000000 and the PIR range is from 1 to 80000000000. You can optionally set an extended burst (BE) size. The BE range is from 1 to 512000000. The default CIR unit is bps, the default PIR unit is **bps**, and the default BE size unit is **bytes**. **Note** You can specify the BC, conform action, and PIR for the same CIR.
Step 8	(Optional) **logging drop threshold** [*drop-count* [**level** *syslog-level*]] **Example:** `switch(config-pmap-c)# logging drop threshold 100`	Specifies the threshold value for dropped packets and generates a syslog if the drop count exceeds the configured threshold. The range for the *drop-count* argument is from 1 to 80000000000 bytes. The range for the *syslog-level* argument is from 1 to 7, and the default level is 4.
Step 9	(Optional) **set cos** [**inner**] *cos-value* **Example:** `switch(config-pmap-c)# set cos 1`	Specifies the 802.1Q class of service (CoS) value. Use the **inner** keyword in a Q-in-Q environment. The range is from 0 to 7. The default value is 0.
Step 10	(Optional) **set dscp** [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default**} **Example:** `switch(config-pmap-c)# set dscp 10`	Specifies the differentiated services code point value in IPv4 and IPv6 packets. Use the **tunnel** keyword to set tunnel encapsulation. The range is from 0 to 63. The default value is 0.
Step 11	(Optional) **set precedence** [**tunnel**] {*prec-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**} **Example:** `switch(config-pmap-c)# set precedence 2`	Specifies the precedence value in IPv4 and IPv6 packets. Use the **tunnel** keyword to set tunnel encapsulation. The range is from 0 to 7. The default value is 0.

Step 12	**exit**
	Example:
	`switch(config-pmap-c)# exit`
	`switch(config-pmap)#`
		Exits policy map class configuration mode.

	Command or Action	Purpose

Step 13	**exit**
	Example:
	`switch(config-pmap)# exit`
	`switch(config)#`
		Exits policy map configuration mode.

Step 14	(Optional) **show policy-map type control-plane** [**expand**] [**name** *class-map-name*] **Example:** `switch(config)# show policy-map type control-plane`	Displays the control plane policy map configuration.
Step 15	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Configuring a Control Plane Class Map, on page 640

Configuring the Control Plane Service Policy

You can configure one or more policy maps for the CoPP service policy.

Before you begin

Ensure that you are in the default VDC.

Ensure that you have configured a control plane policy map.

SUMMARY STEPS

1. **configure terminal**
2. **control-plane**
3. **service-policy input** *policy-map-name*
4. **exit**
5. (Optional) **show running-config copp** [**all**]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**control-plane** **Example:**	Enters control plane configuration mode.

	Command or Action	Purpose
	`switch(config)# control-plane` `switch(config-cp)#`	
Step 3	**service-policy input** *policy-map-name* **Example:** `switch(config-cp)# service-policy input PolicyMapA`	Specifies a policy map for the input traffic. Repeat this step if you have more than one policy map. Use the **no service-policy input** *policy-map-name* command to remove the policy from the control plane.

Step 4	**exit**
	Example:
	`switch(config-cp)# exit`
	`switch(config)#`
		Exits control plane configuration mode.

Step 5	(Optional) **show running-config copp** [**all**] **Example:** `switch(config)# show running-config copp`	Displays the CoPP 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.

Related Topics

Configuring a Control Plane Policy Map, on page 642

Configuring the CoPP Scale Factor Per Line Card

You can configure the CoPP scale factor per line card.

The scale factor configuration is used to scale the policer rate of the applied CoPP policy for a particular line card. The accepted value is from 0.10 to 2.00. You can increase or reduce the policer rate for a particular line card without changing the current CoPP policy. The changes are effective immediately, so you do not need to reapply the CoPP policy.

Note CoPP programming is performed on the forwarding engines of each I/O module. The Cisco Nexus 7000 M Series I/O modules can contain 1 or 2 forwarding engines and the Cisco Nexus7000 F Series modules can contain from 6 to 12 forwarding engines, depending on the module.

If the same CoPP policy profile (strict) that is used for M Series modules is applied on the F Series modules, the traffic that comes to the supervisor from the F Series modules can be many times more than the traffic that comes from the M Series modules and can overwhelm the supervisor. To avoid overwhelming the supervisor, you can configure the dense CoPP profile for F Series modules and certain combinations of F and M Series modules.

Follow these guidelines for configuring the scale factor per I/O module and for applying the appropriate CoPP policy profile, based on the installed I/O modules:

- When a chassis is fully loaded with F Series modules, we recommend that you apply the dense profile without any scale-factor configuration.
- When a chassis is fully loaded with M Series modules, we recommend that you apply the strict profile without any scale-factor configuration.
- When a chassis is loaded with more F series line cards than M series line cards, we recommend that you apply the dense profile and configure a scale-factor value 2 only on the M series line cards.
- When a chassis is loaded with more M series line cards than F series line cards, we recommend that you apply the strict profile and configure a scale-factor value 0.4 only on the F series line cards.

Before you begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. **configure terminal**
2. **control-plane**
3. **scale-factor** *value* **module** *multiple-module-range*
4. (Optional) **show running-config copp** [**all**]
5. (Optional) **show policy-map interface control-plane** [**class** *class-map* | **module** *slot*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**control-plane** **Example:**	Enters control plane configuration mode.

	Command or Action	Purpose
	`switch(config)# control-plane` `switch(config-cp)#`	
Step 3	**scale-factor** *value* **module** *multiple-module-range* **Example:** `switch(config-cp)# scale-factor 1.10 module 1-2`	Configures the policer rate per line card. The allowed scale factor value is from 0.10 to 2.00. When the scale factor value is configured, the policing values are multiplied by the corresponding scale factor value of the module, and it is programmed in the particular module. To revert to the default scale factor value of 1.00, use the **no scale-factor** *value* **module** *multiple-module-range* command, or explicitly set the default scale factor value to 1.00 using the **scale-factor 1 module** *multiple-module-range* command.
Step 4	(Optional) **show running-config copp** [**all**] **Example:** `switch(config-cp)# show running-config copp`	Displays the CoPP configuration in the running configuration.
Step 5	(Optional) **show policy-map interface control-plane** [**class** *class-map* | **module** *slot*] **Example:** `switch(config-cp)# show policy-map interface control-plane`	Displays the applied scale factor values when a CoPP policy is applied.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Changing or Reapplying the Default CoPP Policy

You can change to a different default CoPP policy, or you can reapply the same default CoPP policy.

Note In Cisco NX-OS releases prior to 5.2, you must use the setup utility to change or reapply the default CoPP policy. You can access the setup utility using the **setup** command.

SUMMARY STEPS

1. [**no**] **copp profile** [**strict** | **moderate** | **lenient** | **dense**]
2. (Optional) **show copp status**
3. (Optional) **show running-config copp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	[**no**] **copp profile** [**strict** | **moderate** | **lenient** | **dense**] **Example:** `switch(config)# copp profile moderate`	Applies the CoPP best practice policy.
Step 2	(Optional) **show copp status** **Example:** `switch(config)# show copp status`	Displays the CoPP status, including the last configuration operation and its status. This command also enables you to verify that the CoPP best practice policy is attached to the control plane.
Step 3	(Optional) **show running-config copp** **Example:** `switch(config)# show running-config copp`	Displays the CoPP configuration in the running configuration.

Related Topics

Changing or Reapplying the Default CoPP Policy Using the Setup Utility, on page 660

Copying the CoPP Best Practice Policy

The CoPP best practice policy is read-only, beginning with Cisco NX-OS Release 5.2. If you want to modify its configuration, you must copy it.

SUMMARY STEPS

1. **copp copy profile** {**strict** | **moderate** | **lenient** | **dense**} {**prefix** | **suffix**} *string*
2. (Optional) **show copp status**
3. (Optional) **show running-config copp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**copp copy profile** {**strict** | **moderate** | **lenient** | **dense**} {**prefix** | **suffix**} *string* **Example:** `switch# copp copy profile strict prefix abc`	Creates a copy of the CoPP best practice policy. CoPP renames all class maps and policy maps with the specified prefix or suffix.
Step 2	(Optional) **show copp status** **Example:** `switch# show copp status`	Displays the CoPP status, including the last configuration operation and its status. This command also enables you to verify that the copied policy is not attached to the control plane.
Step 3	(Optional) **show running-config copp** **Example:** `switch# show running-config copp`	Displays the CoPP configuration in the running configuration, including the copied policy configuration.

Verifying the CoPP Configuration

To display CoPP configuration information, perform one of the following tasks:

Command	Purpose
show policy-map type control-plane [**expand**] [**name** *policy-map-name*]	Displays the control plane policy map with associated class maps and CIR and BC values.
show policy-map interface control-plane [**class** *class-map* | **module** *slot*]	Displays the policy values with associated class maps and drops per policy or class map. It also displays the scale factor values when a CoPP policy is applied. When the scale factor value is the default (1.00), it is not displayed. **Note** The scale factor changes the CIR, BC, PIR, and BE values internally on each module, but the display shows the configured CIR, BC, PIR, and BE values only. The actual applied value on a module is the scale factor multiplied by the configured value.
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.

Command	Purpose
show copp diff profile {**strict** | **moderate** | **lenient** | **dense**} [**prior-ver**] **profile** {**strict** | **moderate** | **lenient** | **dense**}	Displays the difference between two CoPP best practice policies. When you do not include the **prior-ver** option, this command displays the difference between two currently applied default CoPP best practice policies (such as the currently applied strict and currently applied moderate policies). When you include the **prior-ver** option, this command displays the difference between a currently applied default CoPP best practice policy and a previously applied default CoPP best practice policy (such as the currently applied strict and the previously applied lenient policies).
show copp profile {**strict** | **moderate** | **lenient** | **dense**}	Displays the details of the CoPP best practice policy, along with the classes and policer values.
show ip access-lists [*acl-name*]	Displays the access lists, including the ACLs. If the **statistics per-entry** command is used, it also displays hit counts for specific entries.
show running-config aclmgr [**all**]	Displays the user-configured access control lists (ACLs) in the running configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
show running-config copp [**all**]	Displays the CoPP configuration in the running configuration.
show startup-config aclmgr [**all**]	Displays the user-configured access control lists (ACLs) in the startup configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Displaying the CoPP Configuration Status

Before you begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. switch# **show copp status**

DETAILED STEPS

	Command or Action	Purpose
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

Before you begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. switch# **show policy-map interface control-plane** {[**module** *module-number* [**inst-all**]] [**class** {*class-map* | **violated**}] | [**class** {*class-map* | **violated**}] [**module** *module-number* [**inst-all**]]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **show policy-map interface control-plane** {[**module** *module-number* [**inst-all**]] [**class** {*class-map* | **violated**}] | [**class** {*class-map* | **violated**}] [**module** *module-number* [**inst-all**]]}	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).

	Command or Action	Purpose
		Note With Supervisor 3 or F2e Series modules, the output of this command uses Layer 3 packet lengths when displaying the byte count. With M1, M2, or F2 Series modules, the command output uses Layer 2 packet lengths for the byte count.

Example

This example shows how to monitor CoPP:

```
switch# show policy-map interface control-plane
Control Plane
  service-policy input copp-system-p-policy-strict

    class-map copp-system-p-class-critical (match-any)
      match access-group name copp-system-p-acl-bgp
      match access-group name copp-system-p-acl-rip
      match access-group name copp-system-p-acl-vpc
      match access-group name copp-system-p-acl-bgp6
      match access-group name copp-system-p-acl-lisp
      match access-group name copp-system-p-acl-ospf
      match access-group name copp-system-p-acl-rip6
      match access-group name copp-system-p-acl-rise
      match access-group name copp-system-p-acl-eigrp
      match access-group name copp-system-p-acl-lisp6
      match access-group name copp-system-p-acl-ospf6
      match access-group name copp-system-p-acl-rise6
      match access-group name copp-system-p-acl-eigrp6
      match access-group name copp-system-p-acl-otv-as
      match access-group name copp-system-p-acl-mac-l2pt
      match access-group name copp-system-p-acl-mpls-ldp
      match access-group name copp-system-p-acl-mpls-rsvp
      match access-group name copp-system-p-acl-mac-l3-isis
      match access-group name copp-system-p-acl-mac-otv-isis
      match access-group name copp-system-p-acl-mac-fabricpath-isis
      match protocol mpls router-alert
      set cos 7
      police cir 36000 kbps bc 250 ms
        conform action: transmit
        violate action: drop
      module 12:
        conformed 0 bytes,
          5-min offered rate 0 bytes/sec
          peak rate 0 bytes/sec
        violated 0 bytes,
          5-min violate rate 0 bytes/sec
          peak rate 0 bytes/sec
      module 14:
        conformed 0 bytes,
          5-min offered rate 0 bytes/sec
          peak rate 0 bytes/sec
        violated 0 bytes,
          5-min violate rate 0 bytes/sec
          peak rate 0 bytes/sec

    class-map copp-system-p-class-important (match-any)
      match access-group name copp-system-p-acl-cts
```

```
      match access-group name copp-system-p-acl-glbp
      match access-group name copp-system-p-acl-hsrp
      match access-group name copp-system-p-acl-vrrp
      match access-group name copp-system-p-acl-wccp
      match access-group name copp-system-p-acl-hsrp6
      match access-group name copp-system-p-acl-vrrp6
      match access-group name copp-system-p-acl-opflex
      match access-group name copp-system-p-acl-mac-lldp
      match access-group name copp-system-p-acl-mac-mvrp
      match access-group name copp-system-p-acl-mac-flow-control
      set cos 6
      police cir 1400 kbps bc 1500 ms
        conform action: transmit
        violate action: drop
      module 12:
        conformed 0 bytes,
          5-min offered rate 0 bytes/sec
          peak rate 0 bytes/sec
        violated 0 bytes,
          5-min violate rate 0 bytes/sec
          peak rate 0 bytes/sec
      module 14:
        conformed 0 bytes,
          5-min offered rate 0 bytes/sec
          peak rate 0 bytes/sec
        violated 0 bytes,
          5-min violate rate 0 bytes/sec
          peak rate 0 bytes/sec
....
```

This example shows the 5-minute moving averages and peaks of the conformed and violated byte counts in the output of the **show policy-map interface control-plane** command. In this example, the 5-minute offered rate is the 5-minute moving average of the conformed bytes, the 5-minute violate rate is the 5-minute moving average of the violated bytes, and the peak rate is the highest value since boot-up or counter reset.

```
class-map copp-system-p-class-multicast-router (match-any)
      match access-group name copp-system-p-acl-pim
      match access-group name copp-system-p-acl-msdp
      match access-group name copp-system-p-acl-pim6
      match access-group name copp-system-p-acl-pim-reg
      match access-group name copp-system-p-acl-pim6-reg
      match access-group name copp-system-p-acl-pim-mdt-join
      match protocol mpls exp 6
      set cos 6
      police cir 2600 kbps bc 1000 ms
        conform action: transmit
        violate action: drop
      module 12:
        conformed 0 bytes,
          5-min offered rate 0 bytes/sec
          peak rate 0 bytes/sec
        violated 0 bytes,
          5-min violate rate 0 bytes/sec
          peak rate 0 bytes/sec
      module 14:
        conformed 0 bytes,
          5-min offered rate 0 bytes/sec
          peak rate 0 bytes/sec
        violated 0 bytes,
          5-min violate rate 0 bytes/sec
          peak rate 0 bytes/sec
```

This example displays the output of strict profile policy:

```
switch# show copp profile strict
ip access-list copp-system-p-acl-bgp
  permit tcp any gt 1024 any eq bgp
  permit tcp any eq bgp any gt 1024
ipv6 access-list copp-system-p-acl-bgp6
  permit tcp any gt 1024 any eq bgp
  permit tcp any eq bgp any gt 1024
ip access-list copp-system-p-acl-cts
  permit tcp any any eq 64999
  permit tcp any eq 64999 any
ip access-list copp-system-p-acl-dhcp
  permit udp any eq bootpc any
  permit udp any neq bootps any eq bootps
ip access-list copp-system-p-acl-dhcp-relay-response
  permit udp any eq bootps any
  permit udp any any eq bootpc
ipv6 access-list copp-system-p-acl-dhcp6
  permit udp any eq 546 any
  permit udp any neq 547 any eq 547
ipv6 access-list copp-system-p-acl-dhcp6-relay-response
  permit udp any eq 547 any
  permit udp any any eq 546
ip access-list copp-system-p-acl-eigrp
  permit eigrp any any
ipv6 access-list copp-system-p-acl-eigrp6
  permit eigrp any any
ip access-list copp-system-p-acl-ftp
  permit tcp any any eq ftp-data
  permit tcp any any eq ftp
  permit tcp any eq ftp-data any
  permit tcp any eq ftp any
ip access-list copp-system-p-acl-glbp
  permit udp any eq 3222 224.0.0.0/24 eq 3222
ip access-list copp-system-p-acl-hsrp
  permit udp any 224.0.0.2/32 eq 1985
  permit udp any 224.0.0.102/32 eq 1985
ipv6 access-list copp-system-p-acl-hsrp6
  permit udp any ff02::66/128 eq 2029
ip access-list copp-system-p-acl-http-response
  permit tcp any eq 80 any gt 1024
  permit tcp any eq 443 any gt 1024
ipv6 access-list copp-system-p-acl-http6-response
  permit tcp any eq 80 any gt 1024
  permit tcp any eq 443 any gt 1024
ip access-list copp-system-p-acl-icmp
  permit icmp any any echo
  permit icmp any any echo-reply
ipv6 access-list copp-system-p-acl-icmp6
  permit icmp any any echo-request
  permit icmp any any echo-reply
ip access-list copp-system-p-acl-igmp
  permit igmp any 224.0.0.0/3
ip access-list copp-system-p-acl-lisp
  permit udp any any eq 4342
  permit udp any eq 4342 any
ipv6 access-list copp-system-p-acl-lisp6
  permit udp any any eq 4342
  permit udp any eq 4342 any
mac access-list copp-system-p-acl-mac-cdp-udld-vtp
  permit any 0100.0ccc.cccc 0000.0000.0000
mac access-list copp-system-p-acl-mac-cfsoe
  permit any 0180.c200.000e 0000.0000.0000 0x8843
```

```
  permit any 0180.c200.000e 0000.0000.0000
mac access-list copp-system-p-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e
mac access-list copp-system-p-acl-mac-ecp-ack
  permit any 0180.c200.0000 0000.0000.0000 0x8940
  permit 0180.c200.0000 0000.0000.0000 any 0x8940
  permit any any 0x8940
```

Monitoring CoPP with SNMP

Beginning with Cisco NX-OS Release 6.2(2), CoPP supports the Cisco class-based QoS MIB (cbQoSMIB). All of the CoPP elements can now be monitored (but not modified) using SNMP. This feature applies only to policies and their subelements (such as classes, match rules, and set actions) that are attached to the control plane. Elements of policies that are not in service on the control plane are not visible through SNMP.

The following cbQoSMIB tables are supported:

- ccbQosServicePolicy
- cbQosInterfacePolicy
- cbQosObjects
- cbQosPolicyMapCfg
- cbQosClassMapCfg
- cbQosMatchStmtCfg
- cbQosPoliceCfg
- cbQosSetCfg

More detailed information on cbQoSMIB tables and elements is available at the following urls:

- http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.4.1.9.9.166
- http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus6000/sw/system_management/7x/b_6k_System_Mgmt_Config_7x/b_6k_System_Mgmt_Config_7x_chapter_010110.html

Clearing the CoPP Statistics

Before you begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. (Optional) switch# **show policy-map interface control-plane** [**class** *class-map* | **module** *slot*]
2. switch# **clear copp statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) switch# **show policy-map interface control-plane** [**class** *class-map* | **module** *slot*]	Displays the currently applied CoPP policy and per-class statistics.
Step 2	switch# **clear copp statistics**	Clears the CoPP statistics.

Example

This example shows how to clear the CoPP statistics for your installation:

```
switch# show policy-map interface control-plane
switch# clear copp statistics
```

Configuration Examples for CoPP

This section includes example CoPP configurations.

CoPP Configuration Example

The following example shows how to configure CoPP using IP ACLs and MAC ACLs:

```
configure terminal
ip access-list copp-system-acl-igmp
permit igmp any 10.0.0.0/24

ip access-list copp-system-acl-msdp
permit tcp any any eq 639

mac access-list copp-system-acl-arp
permit any any 0x0806

ip access-list copp-system-acl-tacas
permit udp any any eq 49

ip access-list copp-system-acl-gre
permit 47 any any

ip access-list copp-system-acl-ntp
permit udp any 10.0.1.1/23 eq 123

ip access-list copp-system-acl-icmp
permit icmp any any

class-map type control-plane match-any copp-system-class-critical
match access-group name copp-system-acl-igmp
match access-group name copp-system-acl-msdp

class-map type control-plane match-any copp-system-class-important
match access-group name copp-system-acl-gre

class-map type control-plane match-any copp-system-class-normal
match access-group name copp-system-acl-icmp
```

```
match exception ip icmp redirect
match exception ip icmp unreachable
match exception ip option
match redirect arp-inspect
match redirect dhcp-snoop

policy-map type control-plane copp-system-policy

class copp-system-class-critical
police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

class copp-system-class-important
police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

class copp-system-class-normal
police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

class class-default
police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

control-plane
service-policy input copp-system-policy
```

The following example shows how to create the CoPP class and associate an ACL:

```
class-map type control-plane copp-arp-class
match access-group name copp-arp-acl
```

The following example shows how to add the class to the CoPP policy:

```
policy-map type control-plane copp-system-policy
class copp-arp-class
police pps 500
```

Preventing CoPP Overflow by Splitting ICMP Pings and ARP Requests

Some servers use ICMP pings and ARP requests to the default gateway to verify that the active NIC still has access to the aggregation switch. As a result, if the CoPP values are exceeded, CoPP starts dropping traffic for all networks. One malfunctioning server can send out thousands of ICMP pings and ARP requests, causing all servers in one aggregation block to lose their active NIC and start swapping NICs.

If your server is configured as such, you can minimize the CoPP overflow by splitting the ICMP pings and ARP requests based on subnets or groups of subnets. Then if a server malfunctions and overflows CoPP, the supervisor answers the ICMP pings and ARP requests only on some subnetworks.

The last entry in the class map or policy map should identify all of the ICMP pings and ARP requests in the networks that are not specified. If these counters increase, it means that a new network was added that was not specified in the existing ACLs for ICMP and ARP. In this case, you would need to update the ACLs related to ICMP and ARP.

Note Per the default CoPP, ICMP pings fall under copp-system-p-class-monitoring, and ARP requests fall under copp-system-p-class-normal.

The following example shows how to prevent a CoPP overflow by splitting ICMP and ARP requests.

First, add the new ACLs that identify the networks you want to group together based on the findings of the investigations of the applications:

```
arp access-list copp-arp-1
statistics per-entry
10 permit ip 10.1.1.0 255.255.255.0 mac any
20 permit ip 10.1.2.0 255.255.255.0 mac any
30 permit ip 10.1.3.0 255.255.255.0 mac any
arp access-list copp-arp-2
statistics per-entry
10 permit ip 10.2.1.0 255.255.255.0 mac any
20 permit ip 10.2.2.0 255.255.255.0 mac any
30 permit ip 10.2.3.0 255.255.255.0 mac any
arp access-list copp-arp-3
statistics per-entry
10 permit ip 10.3.1.0 255.255.255.0 mac any
20 permit ip 10.3.2.0 255.255.255.0 mac any
30 permit ip 10.3.3.0 255.255.255.0 mac any
...
arp access-list copp-arp-10
10 permit ip any any mac any

ip access-list copp-icmp-1
statistics per-entry
10 permit icmp 10.2.1.0 255.255.255.0 any
20 permit icmp 10.2.2.0 255.255.255.0 any
30 permit icmp 10.2.3.0 255.255.255.0 any
ip access-list copp-icmp-2
statistics per-entry
10 permit icmp 10.3.1.0 255.255.255.0 any
10 permit icmp 10.3.2.0 255.255.255.0 any
10 permit icmp 10.3.3.0 255.255.255.0 any
ip access-list copp-icmp-3
statistics per-entry
10 permit icmp 10.4.1.0 255.255.255.0 any
10 permit icmp 10.4.2.0 255.255.255.0 any
10 permit icmp 10.4.3.0 255.255.255.0 any
...
ip access-list copp-icmp-10
10 permit icmp any any
```

Add these ACLs to the new class maps for CoPP:

```
class-map type control-plane match-any copp-cm-arp-1
 match access-group name copp-arp-1
class-map type control-plane match-any copp-cm-arp-2
 match access-group name copp-arp-2
class-map type control-plane match-any copp-cm-arp-3
 match access-group name copp-arp-3
...
class-map type control-plane match-any copp-cm-arp-10
 match access-group name copp-arp-10# class-map type control-plane match-any copp-cm-icmp-1

 match access-group name copp-icmp-1
class-map type control-plane match-any copp-cm-icmp-2
 match access-group name copp-icmp-2
class-map type control-plane match-any copp-cm-icmp-3
 match access-group name copp-icmp-3
...
class-map type control-plane match-any copp-cm-icmp-10
 match access-group name copp-icmp-10
```

Modify the CoPP policy map by adding new policies with the above created class maps:

```
policy-map type control-plane copp-system-p-policy
class copp-cm-icmp-1
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-2
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-3
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-4
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-10
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-1
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-2
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-3
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-4
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-10
      police cir X kbps bc X ms conform transmit violate drop
```

Delete ICMP and ARP from the existing class maps:

```
class-map type control-plane match-any copp-system-p-class-normal
no match protocol arp

class-map type control-plane match-any copp-system-p-class-monitoring
no match access-grp name copp-system-p-acl-icmp
```

Changing or Reapplying the Default CoPP Policy Using the Setup Utility

The following example shows how to change or reapply the default CoPP policy using the setup utility.

Note Beginning with Cisco NX-OS Release 5.2, you can change or reapply the default CoPP policy using the **copp profile** command.

```
switch# setup

         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.


*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.


Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
```

```
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes

Do you want to enforce secure password standard (yes/no)[y]: <CR>

  Create another login account (yes/no) [n]: n

  Configure read-only SNMP community string (yes/no) [n]: n

  Configure read-write SNMP community string (yes/no) [n]: n

  Enter the switch name : <CR>

  Enable license grace period? (yes/no) [n]: n

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: n

  Configure the default gateway? (yes/no) [y]: n

  Configure advanced IP options? (yes/no) [n]: <CR>

  Enable the telnet service? (yes/no) [n]: y

  Enable the ssh service? (yes/no) [y]: <CR>

    Type of ssh key you would like to generate (dsa/rsa) : <CR>

  Configure the ntp server? (yes/no) [n]: n

  Configure default interface layer (L3/L2) [L3]: <CR>

  Configure default switchport interface state (shut/noshut) [shut]: <CR>

  Configure best practices CoPP profile (strict/moderate/lenient/dense/skip) [strict]:
strict

  Configure CMP processor on current sup (slot 6)? (yes/no) [y]: n

  Configure CMP processor on redundant sup (slot 5)? (yes/no) [y]: n

The following configuration will be applied:
  password strength-check
  no license grace-period
  no telnet server enable
  no system default switchport
  system default switchport shutdown
  policy-map type control-plane copp-system-p-policy

Would you like to edit the configuration? (yes/no) [n]: <CR>

Use this configuration and save it? (yes/no) [y]: y

switch#
```

Additional References for CoPP

This section provides additional information related to implementing CoPP.

Related Documents

Related Topic	Document Title
Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

Standards

Standards	Title
RFC 2698	A Two Rate Three Color Marker

Feature History for CoPP

This table lists the release history for this feature.

Table 50: Feature History for CoPP

Feature Name	Releases	Feature Information
CoPP	8.2(6)	Support for uRPF exception CoPP class is introduced.
CoPP	6.2(2)	Updated the output of the **show policy-map interface control-plane** command to show the 5-minute moving averages and peaks of the conformed and violated byte counts for each policy in each module.
CoPP	6.2(2)	Added VRRP6 ACL support to police VRRP IPv6 traffic. The HSRP ACL is modified to reflect the correct destination addresses of control packets.
CoPP	6.2(2)	Changed the behavior of multicast traffic from being policed at different rates in different classes to being grouped into three classes (multicast-host, multicast-router, and normal) and policed at consistent rates.

Feature Name	Releases	Feature Information
CoPP	6.2(2)	Added the ability to monitor CoPP with SNMP.
CoPP	6.1(1)	Added a new class for FCoE; added the LISP, LISP6, and MAC Layer 3 IS-IS ACLs to the critical class; added the fcoe-fib-miss match exception to the undesirable class; added the MAC Layer 2 tunnel ACL to the Layer 2 unpoliced class, and added the "permit icmp any any 143" rule to the acl-icmp6-msgs ACL.
CoPP	6.0(1)	Added the dense default CoPP policy.
CoPP	6.0(1)	Added the ability to configure the CoPP scale factor per line card.
CoPP	5.2(1)	Added the ability to change or reapply the default CoPP policy without rerunning the setup utility.
CoPP	5.2(1)	Changed the CoPP best practice policy to read-only and added the ability to copy the policy in order to modify it.
CoPP	5.2(1)	Added the **show copp profile** and **show copp diff profile** commands to display the details of the CoPP best practice policy and the differences between policies, respectively.
CoPP	5.2(1)	Changed the **show running-config aclmgr** and **show startup-config aclmgr** commands to display only the user-configured ACLs (and not also the default CoPP-configured ACLs) in the running and startup configurations.

Feature Name	Releases	Feature Information
CoPP	5.2(1)	Changed the **show copp status** command to display which flavor of the CoPP best practice policy is attached to the control plane.
CoPP	5.2(1)	Changed the name of the **none** option for the best practices CoPP profile in the setup utility to **skip**.
CoPP	5.2(1)	Updated the default class maps with support for MPLS LDP, MPLS OAM, MPLS RSVP, DHCP relay, and OTV-AS.
Control plane policy map	5.1(1)	Added the ability to specify the threshold value for dropped packets and generate a syslog if the drop count exceeds the configured threshold.
CoPP	5.1(1)	Updated the default policies with the 802.1Q class of service (cos) values.
CoPP	5.1(1)	Added support for non-IP traffic classes.
CoPP	5.0(2)	Updated the default policies with support for ACL HSRP6.
CoPP	4.2(3)	Updated the default policies with support for ACL DHCP.
CoPP	4.2(1)	Updated the default policies with support for WCCP and Cisco TrustSec.

CHAPTER 26

Configuring Rate Limits

This chapter describes how to configure rate limits for supervisor-bound traffic on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Information About Rate Limits

Rate limits can prevent redirected packets for exceptions from overwhelming the supervisor module on a Cisco NX-OS device. You can configure rate limits in packets per second for the following types of redirected packets:

- Access-list log packets
- Data and control packets copied to the supervisor module

- F1 Series module packets
    - rl-1 STP and Fabricpath-ISIS
    - rl-2 L3-ISIS and OTV-ISIS
    - rl-3 UDLD, LACP, CDP and LLDP
    - rl-4 Q-in-Q and ARP request
    - rl-5 IGMP, NTP, DHCP-Snoop, Port-Security and Mgmt traffic
- Layer 2 Tunneling Protocol (L2TP) packets
- Layer 2 multicast-snooping packets
- Layer 2 port-security packets
- Layer 2 storm-control packets
- Layer 2 virtual port channel (vPC) low packets
- Layer 3 control packets
- Layer 3 glean packets
- Layer 3 glean fast-path packets
- Layer 3 maximum transmission unit (MTU) check failure packets
- Layer 3 multicast data packets
- Layer 3 Time-to-Live (TTL) check failure packets
- Receive packets

Beginning in Cisco NX-OS Release 5.1, you can also configure rate limits for packets that reach the supervisor module.

Virtualization Support for Rate Limits

You can configure rate limits only in the default virtual device context (VDC), but the rate limits configuration applies to all VDCs on the Cisco NX-OS device. For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Guidelines and Limitations for Rate Limits

The rate limits feature has the following configuration guidelines and limitations:

- You can set rate limits for supervisor-bound exception and redirected traffic. Use control plane policing (CoPP) for other types of supervisor-bound traffic.

Note Hardware rate limiters protect the supervisor CPU from excessive inbound traffic. The traffic rate allowed by the hardware rate-limiters is configured globally and applied to each individual I/O module. The resulting allowed rate depends on the number of I/O modules in the system. CoPP provides more granular supervisor CPU protection by utilizing the modular quality-of-service CLI (MQC).

- F1 Series modules support up to five rate limiters shared among all control traffic sent to the Supervisor module.

Note F2 Series modules do not support the five F1 Series module rate limiters.

- On F2, M1 and M2 Series modules, IP redirects will be rate limited according to the Layer 3 Time-to-Live (TTL) rate limit configured.

Note 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.

In setting hardware rate-limiter for more than one module, the module level rate-limiter has higher precedence over system level.

Related Topics

Configuring Control Plane Policing, on page 619

Default Settings for Rate Limits

This table lists the default settings for rate limits parameters.

Table 51: Default Rate Limits Parameters Settings

Parameters	Default
Access-list log packets rate limit	100 packets per second
Copy packets rate limit	30,000 packets per second

Parameters	Default
F1 Series module rate limit	RL-1: 4,500 packets per second RL-2: 1,000 packets per second RL-3: 1,000 packets per second RL-4: 100 packets per second RL-5: 1,500 packets per second **Note** These F1 Series module rate limits do not apply to F2 Series modules.
Layer 2 L2TP packets rate limit	4,096 packets per second
Layer 2 multicast-snooping packets rate limit	10,000 packets per second
Layer 2 port-security packets rate limit	Disabled
Layer 2 storm-control packets rate limit	Disabled
Layer 2 VPC low packets rate limit	4,000 packets per second
Layer 3 control packets rate limit	10,000 packets per second
Layer 3 glean packets rate limit	100 packets per second
Layer 3 glean fast-path rate limit	100 packets per second
Layer 3 MTU packets rate limit	500 packets per second
Layer 3 Time-to-Live (TTL) packets rate limit	500 packets per second
Receive packets rate limit	30,000 packets per second
Supervisor packets rate limit	10,000 packets per second

Configuring Rate Limits

You can set rate limits on supervisor-bound traffic.

SUMMARY STEPS

1. **configure terminal**
2. **hardware rate-limiter access-list-log** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
3. **hardware rate-limiter copy** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
4. **hardware rate-limiter f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5** {*packets* | **disable**}} [**module** *module* [**port** *start end*]]
5. **hardware rate-limiter layer-2 l2pt** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
6. **hardware rate-limiter layer-2 mcast-snooping** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
7. **hardware rate-limiter layer-2 port-security** {*packets* | **disable**} [**module** *module* [**port** *start end*]]

8. **hardware rate-limiter layer-2 storm-control** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
9. **hardware rate-limiter layer-2 vpc-low** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
10. **hardware rate-limiter layer-3 control** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
11. **hardware rate-limiter layer-3 glean** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
12. **hardware rate-limiter layer-3 glean-fast** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
13. **hardware rate-limiter layer-3 mtu** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
14. **hardware rate-limiter layer-3 multicast** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
15. **hardware rate-limiter layer-3 ttl** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
16. **hardware rate-limiter receive** {*packets* | **disable**} [**module** *module* [**port** *start end*]]
17. **exit**
18. (Optional) **show hardware rate-limiter** [**access-list-log** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} | **layer-2** {**l2pt** | **mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **module** *module* | **receive**]
19. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**hardware rate-limiter access-list-log** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter access-list-log 200`	Configures rate limits in packets per second for packets copied to the supervisor module for access list logging. The range is from 0 to 30000.
Step 3	**hardware rate-limiter copy** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter copy 30000`	Configures rate limits in packets per second for data and control packets copied to the supervisor module. The range is from 0 to 30000. **Note** Layer 3 control, multicast direct-connect, and ARP request packets are controlled by the Layer 2 copy rate limiter. The first two types of packets are also controlled by Layer 3 rate limiters, and the last two types are also subject to control plane policing (CoPP).
Step 4	**hardware rate-limiter f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5** {*packets* | **disable**}} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter f1 rl-1 1000`	Configures rate limits in packets per second for F1 Series module packets. The range is from 0 to 30000. **Note** The **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} rate limiters are the only rate limiters that are supported on F1 Series modules. The other rate limiters are applicable only to the F2 Series and M1 Series modules.

	Command or Action	Purpose
Step 5	**hardware rate-limiter layer-2 l2pt** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-2 l2pt 30000`	Configures rate limits in packets per second for Layer 2 tunnel protocol packets. The range is from 0 to 30000.
Step 6	**hardware rate-limiter layer-2 mcast-snooping** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-2 mcast-snooping 20000`	Configures rate limits in packets per second for Layer 2 multicast-snooping packets. The range is from 0 to 30000.
Step 7	**hardware rate-limiter layer-2 port-security** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-2 port-security 100000`	Configures rate limits in packets per second for port-security packets. The range is from 0 to 30000.
Step 8	**hardware rate-limiter layer-2 storm-control** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-2 storm-control 10000`	Configures rate limits in packets per second for broadcast, multicast, and unknown unicast storm-control traffic. The range is from 0 to 30000.
Step 9	**hardware rate-limiter layer-2 vpc-low** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-2 vpc-low 10000`	Configures rate limits in packets per second for Layer 2 control packets over the VPC low queue. The range is from 0 to 30000.
Step 10	**hardware rate-limiter layer-3 control** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-3 control 20000`	Configures rate limits in packets per second for Layer 3 control packets. The range is from 0 to 30000.
Step 11	**hardware rate-limiter layer-3 glean** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-3 glean 200`	Configures rate limits in packets per second for Layer 3 glean packets. The range is from 0 to 30000.
Step 12	**hardware rate-limiter layer-3 glean-fast** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-3 glean-fast 500`	Configures rate limits in packets per second for Layer 3 glean fast-path packets. This command sends packets to the supervisor from F2e, M1, or M2 Series modules. The range is from 0 to 30000.

	Command or Action	Purpose
		Glean fast path optimizes the processing of glean packets by the supervisor. Specifically, the line card provides the information needed to trigger an ARP within the packet and relieves the supervisor from having to look up this information. The packets sent to the supervisor using the glean fast path are rate limited **Note** Glean fast path is enabled by default. If glean fast-path programming does not occur due to adjacency resource exhaustion, the system falls back to regular glean programming.
Step 13	**hardware rate-limiter layer-3 mtu** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-3 mtu 1000`	Configures rate limits in packets per second for Layer 3 MTU failure redirected packets. The range is from 0 to 30000.
Step 14	**hardware rate-limiter layer-3 multicast** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-3 multicast 20000`	Configures rate limits in packets per second for Layer 3 multicast packets in packets per second. The range is from 0 to 30000.
Step 15	**hardware rate-limiter layer-3 ttl** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter layer-3 ttl 1000`	Configures rate limits in packets per second for Layer 3 failed Time-to-Live redirected packets. The range is from 0 to 30000.
Step 16	**hardware rate-limiter receive** {*packets* | **disable**} [**module** *module* [**port** *start end*]] **Example:** `switch(config)# hardware rate-limiter receive 40000`	Configures rate limits in packets per second for packets redirected to the supervisor module. The range is from 0 to 30000.

Step 17	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 18	(Optional) **show hardware rate-limiter** [**access-list-log** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} | **layer-2** {**l2pt** | **mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **module** *module* | **receive**] **Example:** `switch# show hardware rate-limiter`	Displays the rate limit configuration.

	Command or Action	Purpose
Step 19	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Rate Limits for Packets That Reach the Supervisor

Beginning in Cisco NX-OS Release 5.1, you can configure rate limits globally on the device for packets that reach the supervisor module. If the rate of incoming or outgoing packets exceeds the configured rate limit, the device logs a system message but does not drop any packets.

Note You can also configure rate limits for packets that reach the supervisor module on a particular interface. For more information, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **rate-limit cpu direction** {**input** | **output** | **both**} **pps** *packets* **action log**
3. (Optional) **exit**
4. (Optional) **show system internal pktmgr internal control sw-rate-limit**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **rate-limit cpu direction** {**input** | **output** | **both**} **pps** *packets* **action log** **Example:** `switch(config)# rate-limit cpu direction both pps 100 action log`	Configures rate limits in packets per second for packets that reach the supervisor module and logs a system message if the rate of incoming or outgoing packets exceeds the rate limit. The range is from 1 to 100000. The default rate is 10000.
Step 3	(Optional) **exit** **Example:** `switch(config)# exit`	Exits global configuration mode.
Step 4	(Optional) **show system internal pktmgr internal control sw-rate-limit** **Example:**	Displays the inband and outband global rate limit configuration for packets that reach the supervisor module.

	Command or Action	Purpose
	`switch# show system internal pktmgr internal control sw-rate-limit`	
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Monitoring Rate Limits

You can monitor rate limits.

SUMMARY STEPS

1. **show hardware rate-limiter** [**access-list-log** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} | **layer-2** {**l2pt** | **mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **module** *module* | **receive**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show hardware rate-limiter** [**access-list-log**	**copy**	**f1** {**rl-1**	**rl-2**	**rl-3**	**rl-4**	**rl-5**}	**layer-2** {**l2pt**	**mcast-snooping**	**port-security**	**storm-control**	**vpc-low**}	**layer-3** {**control**	**glean**	**glean-fast**	**mtu**	**multicast**	**ttl**}	**module** *module*	**receive**] **Example:** `switch# show hardware rate-limiter layer-3 glean`	Displays the rate limit statistics.

Clearing the Rate Limit Statistics

You can clear the rate limit statistics.

SUMMARY STEPS

1. **clear hardware rate-limiter** {**all** | **access-list-log** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} | **layer-2** {**l2pt** | **mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **receive**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clear hardware rate-limiter** {**all**	**access-list-log**	**copy**	**f1** {**rl-1**	**rl-2**	**rl-3**	**rl-4**	**rl-5**}	**layer-2** {**l2pt**	**mcast-snooping**	**port-security**	**storm-control**	**vpc-low**}	Clears the rate limit statistics.

	Command or Action	Purpose
	| **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **receive**} **Example:** `switch# clear hardware rate-limiter`	

Verifying the Rate Limit Configuration

To display the rate limit configuration information, perform the following tasks:

Command	Purpose
show hardware rate-limiter [**access-list-log** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} | **layer-2** {**l2pt** | **mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **module** *module* | **receive**]	Displays the rate limit configuration.
show system internal pktmgr interface ethernet *slot*/*port*	Displays the inband and outband rate limit configuration for packets that reach the supervisor module on a specific interface.
show system internal pktmgr internal control sw-rate-limit	Displays the inband and outband global rate limit configuration for packets that reach the supervisor module.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuration Examples for Rate Limits

The following example shows how to configure rate limits:

```
switch(config)# hardware rate-limiter layer-3 control 20000
switch(config)# hardware rate-limiter copy 30000
```

The following example shows how to configure rate limits globally on the device for packets that reach the supervisor module:

```
switch(config)# rate-limit cpu direction both pps 1000 action log
switch(config)# show system internal pktmgr internal control sw-rate-limit
inband pps global threshold 1000  outband pps global threshold 1000
```

Additional References for Rate Limits

This section includes additional information related to implementing rate limits.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

Feature History for Rate Limits

This table lists the release history for this feature.

Table 52: Feature History for Rate Limits

Feature Name	Releases	Feature Information	
Rate limits	6.2(2)	Added support for Layer 3 glean fast-path packets.	
Rate limits	6.0(1)	Added support for F2 Series modules.	
Rate limits	5.2(1)	No change from Release 5.1.	
Rate limits	5.1(1)	Added support for F1 Series module packets.	
Rate limits	5.1(1)	Added the ability to configure rate limits for packets that reach the supervisor module and to log a system message if the rate limit is exceeded.	
Rate limits	5.1(1)	Added options to disable rate limits and to configure rate limits for a specific module and port range.	
Rate limits	5.0(2)	Added support for Layer 2 Tunnel Protocol (L2TP) packets.	
Rate limits	4.2(1)	No change from Release 4.1.	