



Cisco Nexus 3548 Switch NX-OS Security Configuration Guide, Release 6.x

First Published: 2013-05-21

Last Modified: 2019-02-28

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

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

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

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

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

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

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

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

© 2013–2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface	xi
Audience	xi
Document Conventions	xi
Documentation Feedback	xii

CHAPTER 1

New and Changed Information	1
New and Changed Information	1

CHAPTER 2

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

CHAPTER 3

Configuring Authentication, Authorization, and Accounting	5
Information About AAA	5
AAA Security Services	5
Benefits of Using AAA	6
Remote AAA Services	6
AAA Server Groups	6
AAA Service Configuration Options	6
Authentication and Authorization Process for User Logins	7
Prerequisites for Remote AAA	9
Guidelines and Limitations for AAA	9
Configuring AAA	9
Configuring Console Login Authentication Methods	9

Configuring Default Login Authentication Methods	11
Enabling Login Authentication Failure Messages	11
Configuring AAA Command Authorization	12
Enabling MSCHAP Authentication	14
Configuring AAA Accounting Default Methods	14
Using AAA Server VSAs	16
VSAs	16
VSA Format	16
Specifying Switch User Roles and SNMPv3 Parameters on AAA Servers	16
Monitoring and Clearing the Local AAA Accounting Log	17
Verifying the AAA Configuration	17
Configuration Examples for AAA	18
Default AAA Settings	18
<hr/>	
CHAPTER 4	Configuring RADIUS 19
Configuring RADIUS	19
Information About RADIUS	19
RADIUS Network Environments	19
Information About RADIUS Operations	20
RADIUS Server Monitoring	20
Vendor-Specific Attributes	21
Prerequisites for RADIUS	22
Guidelines and Limitations for RADIUS	22
Configuring RADIUS Servers	22
Configuring RADIUS Server Hosts	23
Configuring RADIUS Global Preshared Keys	23
Configuring RADIUS Server Preshared Keys	24
Configuring RADIUS Server Groups	25
Configuring the Global Source Interface for RADIUS Server Groups	26
Allowing Users to Specify a RADIUS Server at Login	27
Configuring the Global RADIUS Transmission Retry Count and Timeout Interval	28
Configuring the RADIUS Transmission Retry Count and Timeout Interval for a Server	29
Configuring Accounting and Authentication Attributes for RADIUS Servers	29
Configuring Periodic RADIUS Server Monitoring	30

Configuring the Dead-Time Interval	32
Manually Monitoring RADIUS Servers or Groups	32
Verifying the RADIUS Configuration	33
Displaying RADIUS Server Statistics	33
Clearing RADIUS Server Statistics	33
Configuration Examples for RADIUS	33
Default Settings for RADIUS	34

CHAPTER 5
Configuring TACACS+ 35

About Configuring TACACS+	35
Information About Configuring TACACS+	35
TACACS+ Advantages	35
User Login with TACACS+	36
Default TACACS+ Server Encryption Type and Preshared Key	36
Command Authorization Support for TACACS+ Servers	37
TACACS+ Server Monitoring	37
Prerequisites for TACACS+	37
Guidelines and Limitations for TACACS+	38
Configuring TACACS+	38
TACACS+ Server Configuration Process	38
Displaying TACACS+ Statistics	54
Verifying the TACACS+ Configuration	54
Configuration Examples for TACACS+	55
Default Settings for TACACS+	55

CHAPTER 6
Configuring SSH and Telnet 57

Configuring SSH and Telnet	57
Information About SSH and Telnet	57
SSH Server	57
SSH Client	57
SSH Server Keys	57
Telnet Server	58
Guidelines and Limitations for SSH	58
Configuring SSH	58

Generating SSH Server Keys	58
Specifying the SSH Public Keys for User Accounts	59
Starting SSH Sessions to Remote Devices	61
Clearing SSH Hosts	61
Disabling the SSH Server	62
Deleting SSH Server Keys	62
Clearing SSH Sessions	62
Configuration Examples for SSH	63
Configuring Telnet	64
Enabling the Telnet Server	64
Starting Telnet Sessions to Remote Devices	64
Clearing Telnet Sessions	65
Verifying the SSH and Telnet Configuration	65
Default Settings for SSH	66

CHAPTER 7

Configuring Access Control Lists	67
Information About ACLs	67
IP ACL Types and Applications	67
Application Order	68
Rules	69
Source and Destination	69
Protocols	69
Implicit Rules	69
Additional Filtering Options	69
Sequence Numbers	70
Logical Operators and Logical Operation Units	70
ACL TCAM Regions	71
Licensing Requirements for ACLs	72
Prerequisites for ACLs	72
Guidelines and Limitations for ACLs	72
Default ACL Settings	73
Configuring IP ACLs	74
Creating an IP ACL	74
Changing an IP ACL	74

Removing an IP ACL	75
Changing Sequence Numbers in an IP ACL	76
Applying an IP ACL to mgmt0	76
Applying an IP ACL as a Port ACL	77
Applying an IP ACL as a Router ACL	78
Verifying IP ACL Configurations	79
Monitoring and Clearing IP ACL Statistics	79
Information About VLAN ACLs	80
VACLs and Access Maps	80
VACLs and Actions	80
Statistics	80
Configuring VACLs	81
Creating or Changing a VACL	81
Removing a VACL	81
Applying a VACL to a VLAN	82
Verifying VACL Configuration	82
Displaying and Clearing VACL Statistics	83
Configuration Examples for VACL	83
Configuring ACL TCAM Region Sizes	83
Reverting to the Default TCAM Region Sizes	86
Configuring ACLs on Virtual Terminal Lines	86
Verifying ACLs on VTY Lines	88
Configuration Examples for ACLs on VTY Lines	88

CHAPTER 8
Configuring DHCP Snooping 91

Information About DHCP Snooping	91
Feature Enabled and Globally Enabled	91
Trusted and Untrusted Sources	92
DHCP Snooping Binding Database	93
Information About the DHCP Relay Agent	93
DHCP Relay Agent	93
VRF Support for the DHCP Relay Agent	93
DHCP Relay Binding Database	94
Licensing Requirements for DHCP Snooping	94

Prerequisites for DHCP Snooping	94
Guidelines and Limitations for DHCP Snooping	95
Default Settings for DHCP Snooping	95
Configuring DHCP Snooping	95
Minimum DHCP Snooping Configuration	95
Enabling or Disabling the DHCP Snooping Feature	96
Enabling or Disabling DHCP Snooping Globally	97
Enabling or Disabling DHCP Snooping on a VLAN	97
Enabling or Disabling Option 82 Data Insertion and Removal	98
Enabling or Disabling Option 82 User Defined Data Insertion and Removal	99
Enabling or Disabling Strict DHCP Packet Validation	100
Configuring an Interface as Trusted or Untrusted	101
Enabling or Disabling the DHCP Relay Agent	102
Enabling or Disabling Option 82 for the DHCP Relay Agent	102
Enabling or Disabling VRF Support for the DHCP Relay Agent	103
Enabling or Disabling Subnet Broadcast Support for the DHCP Relay Agent on a Layer 3 Interface	104
Configuring DHCP Server Addresses on an Interface	105
Creating a DHCP Static Binding	107
Verifying the DHCP Snooping Configuration	108
Displaying DHCP Bindings	108
Clearing the DHCP Snooping Binding Database	109
Clearing DHCP Relay Statistics	110
Monitoring DHCP	110
Configuration Examples for DHCP Snooping	110

CHAPTER 9
Configuring MAC ACLs 111

Information About MAC ACLs	111
MAC Packet Classification	111
Default Settings for MAC ACLs	112
Configuring MAC ACLs	112
Creating a MAC ACL	112
Changing a MAC ACL	113
Changing Sequence Numbers in a MAC ACL	114

Removing a MAC ACL	115
Applying a MAC ACL as a Port ACL	116
Enabling or Disabling MAC Packet Classification	118
Verifying the MAC ACL Configuration	118
Clearing MAC ACL Statistics	119

CHAPTER 10**Configuring Unicast RPF 121**

Information About Unicast RPF	121
Unicast RPF	122
Global Statistics	122
Licensing Requirements for Unicast RPF	122
Guidelines and Limitations for Unicast RPF	122
Default Settings for Unicast RPF	123
Configuring Unicast RPF	123
Configuration Examples for Unicast RPF	124
Verifying the Unicast RPF Configuration	125

CHAPTER 11**Configuring Control Plane Policing 127**

Information About CoPP	127
Control Plane Protection	128
Control Plane Packet Types	129
Classification for CoPP	129
Rate Controlling Mechanisms	129
CoPP Policy Templates	130
Default CoPP Policy	130
Layer 2 CoPP Policy	131
Layer 3 CoPP Policy	133
CoPP Class Maps	134
Packets Per Second Credit Limit	135
CoPP and the Management Interface	135
Licensing Requirements for CoPP	135
Guidelines and Limitations for CoPP	135
Upgrade Guidelines for CoPP	137
Configuring CoPP	137

Configuring a Control Plane Class Map	137
Configuring a Control Plane Policy Map	138
Configuring the Control Plane Service Policy	140
CoPP Show Commands	140
Displaying the CoPP Configuration Status	141
Monitoring CoPP	142
Clearing the CoPP Statistics	142
CoPP Configuration Examples	143
Sample CoPP Configuration	145
Example: Changing or Reapplying the Default CoPP Policy Using the Setup Utility	148



Preface

The preface contains the following sections:

- [Audience, on page xi](#)
- [Document Conventions, on page xi](#)
- [Documentation Feedback, on page xii](#)

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.
<i>Italic</i>	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.
{x y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.

Convention	Description
[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.
<i>variable</i>	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
<code>screen font</code>	Terminal sessions and information the switch displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
<i>italic screen font</i>	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.

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.



CHAPTER 1

New and Changed Information

This chapter contains the following sections:

- [New and Changed Information, on page 1](#)

New and Changed Information

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

Table 1: New Features

Feature	Description	Release	Where Documented
New CoPP Class	Added a new CoPP class - copp-s-pim-datareg for PIM protocol	6.0(2)A8(9)	CoPP Class Maps, on page 134 CoPP Configuration Examples, on page 143
DHCP Snooping	Added support for enabling or disabling option 82 for user defined data insertion and removal.	6.0(2)A8(1)	Enabling or Disabling Option 82 User Defined Data Insertion and Removal, on page 99
Configuring Unicast RPF	Describes how to configure rate limits for egress traffic on Cisco NX-OS devices.	6.0(2)A7(1)	Information About Unicast RPF, on page 121

Feature	Description	Release	Where Documented
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. Cisco NX-OS Release 6.0(2)A4(1) introduces support for MAC ACLs on Cisco Nexus 3500 Series switches.	6.0(2)A4(1)	Information About MAC ACLs, on page 111
Static NAT	This chapter has been moved and combined with the Dynamic NAT feature.		Cisco Nexus 3548 Switch NX-OS Interfaces Configuration Guide, Release 6.0(2)A1(1).



CHAPTER 2

Overview

This chapter contains the following sections:

- [Authentication, Authorization, and Accounting, on page 3](#)
- [RADIUS and TACACS+ Security Protocols, on page 4](#)
- [SSH and Telnet, on page 4](#)
- [IP ACLs, on page 4](#)

Authentication, Authorization, and Accounting

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

Authentication

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

Authorization

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

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

Accounting

Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables you to track the services that users are accessing, as well as the amount of network resources that they are consuming.



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.

SSH and Telnet

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

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

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

IP ACLs

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



CHAPTER 3

Configuring Authentication, Authorization, and Accounting

This chapter contains the following sections:

- [Information About AAA, on page 5](#)
- [Prerequisites for Remote AAA, on page 9](#)
- [Guidelines and Limitations for AAA, on page 9](#)
- [Configuring AAA, on page 9](#)
- [Monitoring and Clearing the Local AAA Accounting Log , on page 17](#)
- [Verifying the AAA Configuration, on page 17](#)
- [Configuration Examples for AAA, on page 18](#)
- [Default AAA Settings, on page 18](#)

Information About AAA

AAA Security Services

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

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

AAA security provides the following services:

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

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

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



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

Benefits of Using AAA

AAA provides the following benefits:

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

Remote AAA Services

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

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

AAA Server Groups

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

AAA Service Configuration Options

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

- User Telnet or Secure Shell (SSH) login authentication
- Console login authentication

- User management session accounting

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

Table 2: AAA Service Configuration Commands

AAA Service Configuration Option	Related Command
Telnet or SSH login	aaa authentication login default
Console login	aaa authentication login console
User session accounting	aaa accounting default

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

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



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

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

Table 3: AAA Authentication Methods for AAA Services

AAA Service	AAA Methods
Console login authentication	Server groups, local, and none
User login authentication	Server groups, local, and none
User management session accounting	Server groups and local



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

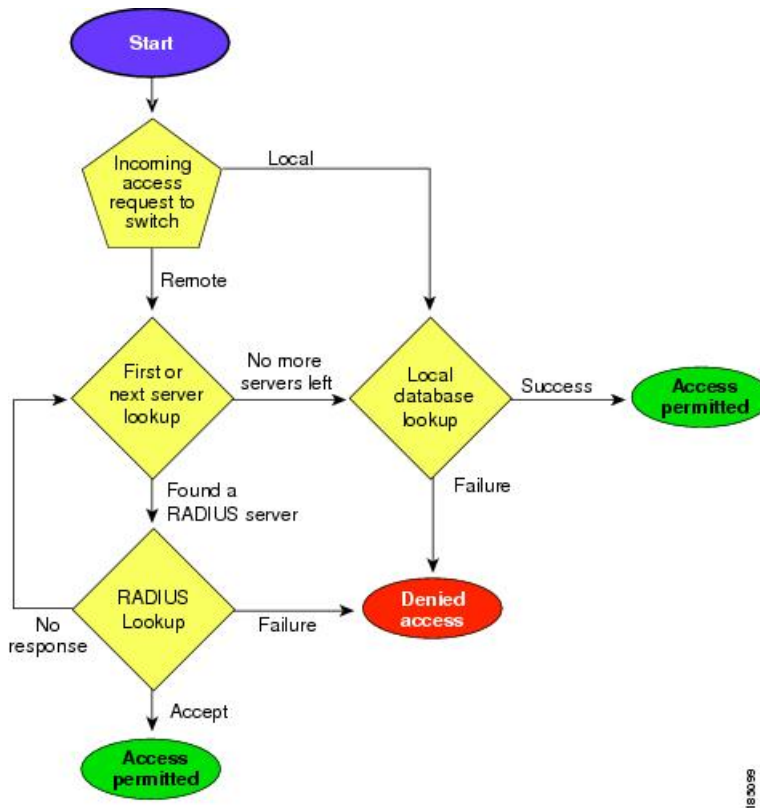
Authentication and Authorization Process for User Logins

The authentication and authorization process for user login is as occurs:

- When you log in to the required Cisco Nexus device, you can use the Telnet, SSH, Fabric Manager or Device Manager, or console login options.
- When you have configured the AAA server groups using the server group authentication method, the Cisco Nexus device sends an authentication request to the first AAA server in the group as follows:
 - If the AAA server fails to respond, then the next AAA server is tried and so on until the remote server responds to the authentication request.
 - If all AAA servers in the server group fail to respond, the servers in the next server group are tried.
 - If all configured methods fail, the local database is used for authentication.
- If a Cisco Nexus device successfully authenticates you through a remote AAA server, the following conditions apply:
 - If the AAA server protocol is RADIUS, user roles specified in the cisco-av-pair attribute are downloaded with an authentication response.
 - If the AAA server protocol is TACACS+, another request is sent to the same server to get the user roles specified as custom attributes for the shell.
- If your username and password are successfully authenticated locally, the Cisco Nexus device logs you in and assigns you the roles configured in the local database.

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

Figure 1: Authentication and Authorization Flow for User Login





Note This figure 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.

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

Prerequisites for Remote AAA

Remote AAA servers have the following prerequisites:

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

Guidelines and Limitations for AAA

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



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

Configuring AAA

Configuring Console Login Authentication Methods

The authentication methods include the following:

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

The default method is local.



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

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

Procedure

	Command or Action	Purpose
Step 1	<code>switch# configure terminal</code>	Enters global configuration mode.
Step 2	<code>switch(config)# aaa authentication login console {group group-list [none] local none}</code>	<p>Configures login authentication methods for the console.</p> <p>The <code>group-list</code> argument consists of a space-delimited list of group names. The group names are the following:</p> <ul style="list-style-type: none"> • radius —Uses the global pool of RADIUS servers for authentication. • named-group —Uses a named subset of TACACS+ or RADIUS servers for authentication. <p>The local method uses the local database for authentication. The none method uses the username only.</p> <p>The default console login method is local, which is used when no methods are configured or when all of the configured methods fail to respond.</p>
Step 3	<code>switch(config)# exit</code>	Exits global configuration mode.
Step 4	(Optional) <code>switch# show aaa authentication</code>	Displays the configuration of the console login authentication methods.
Step 5	(Optional) <code>switch# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Example

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

```
switch# configure terminal
switch(config)# aaa authentication login console group radius
switch(config)# exit
```

```
switch# show aaa authentication
switch# copy running-config startup-config
```

Configuring Default Login Authentication Methods

The default method is local.

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# aaa authentication login default {group group-list [none] local none}	<p>Configures the default authentication methods. The <i>group-list</i> argument consists of a space-delimited list of group names. The group names are the following:</p> <ul style="list-style-type: none"> • radius —Uses the global pool of RADIUS servers for authentication. • named-group —Uses a named subset of TACACS+ or RADIUS servers for authentication. <p>The local method uses the local database for authentication. The none method uses the username only.</p> <p>The default login method is local, which is used when no methods are configured or when all of the configured methods do not respond.</p>
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	(Optional) switch# show aaa authentication	Displays the configuration of the default login authentication methods.
Step 5	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Enabling Login Authentication Failure Messages

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

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

Procedure

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

Configuring AAA Command Authorization

When a TACACS+ server authorization method is configured, you can authorize every command that a user executes with the TACACS+ server which includes all EXEC mode commands and all configuration mode commands.

The authorization methods include the following:

- Group—TACACS+ server group
- Local—Local role-based authorization
- None—No authorization is performed

The default method is Local.

**Note**

Authorization on the console session is not supported on the Cisco Nexus 5000 platform. It is supported on the Cisco Nexus 5500 platform, release 6.x onwards.

Before you begin

You must enable TACACS+ before configuring AAA command authorization.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# <code>configure terminal</code> switch(config)#	Enters global configuration mode.
Step 2	aaa authorization {commands config-commands} {default} {[group	Configures authorization parameters.

	Command or Action	Purpose
	<p><i>group-name</i> [local] {[group <i>group-name</i>] [none]}</p> <p>Example:</p> <pre>switch(config)# aaa authorization config-commands default group tac1</pre> <p>Example:</p> <pre>switch# aaa authorization commands default group tac1</pre>	<p>Use the commands keyword to authorize EXEC mode commands.</p> <p>Use the config-commands keyword to authorize configuration mode commands.</p> <p>Use the group, local, or none keywords to identify the authorization method.</p>

Example

The following example shows how to authorize EXEC mode commands with TACACS+ server group *tac1*:

```
switch# aaa authorization commands default group tac1
```

The following example shows how to authorize configuration mode commands with TACACS+ server group *tac1*:

```
switch(config)# aaa authorization config-commands default group tac1
```

The following example shows how to authorize configuration mode commands with TACACS+ server group *tac1*:

- If the server is reachable, the command is allowed or not allowed based on the server response.
- If there is an error reaching the server, the command is authorized based on the user's *local* role.

```
switch(config)# aaa authorization config-commands default group tac1 local
```

The following example shows how to authorize configuration mode commands with TACACS+ server group *tac1*:

- If the server is reachable, the command is allowed or not allowed based on the server response.
- If there is an error reaching the server, allow the command regardless of the local role.

```
switch# aaa authorization commands default group tac1 none
```

The following example shows how to authorize EXEC mode commands regardless of the local role:

```
switch# aaa authorization commands default none
```

The following example shows how to authorize EXEC mode commands using the local role for authorization:

```
switch# aaa authorization commands default local
```

Enabling MSCHAP Authentication

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

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

The following table describes the RADIUS VSAs required for MSCHAP.

Table 4: MSCHAP 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 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 user in response to the challenge. It is only used in Access-Request packets.

Procedure

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

Configuring AAA Accounting Default Methods

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

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

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

- RADIUS server group—Uses the global pool of RADIUS servers for accounting.

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



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

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# aaa accounting default { group <i>group-list</i> local }	Configures the default accounting method. One or more server group names can be specified in a space-separated list. The <i>group-list</i> argument consists of a space-delimited list of group names. The group names are the following: <ul style="list-style-type: none"> • radius —Uses the global pool of RADIUS servers for accounting. • <i>named-group</i> —Uses a named subset of TACACS+ or RADIUS servers for accounting. <p>The local method uses the local database for accounting.</p> <p>The default method is local, which is used when no server groups are configured or when all the configured server group do not respond.</p>
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	(Optional) switch# show aaa accounting	Displays the configuration AAA accounting default methods.
Step 5	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Using AAA Server VSAs

VSAs

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

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

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

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

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

VSA Format

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

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

The following attributes are supported by the Cisco Nexus device:

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

Specifying Switch User Roles and SNMPv3 Parameters on AAA Servers

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

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

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



Note For information on Cisco Unified Wireless Network TACACS+ configurations and to change the user roles, see [Cisco Unified Wireless Network TACACS+ Configuration](#).

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

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

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

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

Monitoring and Clearing the Local AAA Accounting Log

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

Procedure

	Command or Action	Purpose
Step 1	switch# show accounting log [<i>size</i>] [start-time <i>year month day hh : mm : ss</i>]	Displays the accounting log contents. By default, the command output contains up to 250,000 bytes of the accounting log. You can use the size argument to limit command output. The range is from 0 to 250000 bytes. You can also specify a start time for the log output.
Step 2	(Optional) switch# clear accounting log	Clears the accounting log contents.

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 { error-enable mschap }]	Displays AAA authentication information.
show aaa authorization	Displays AAA authorization 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.

Configuration Examples for AAA

The following example shows how to configure AAA:

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

Default AAA Settings

The following table lists the default settings for AAA parameters.

Table 5: Default AAA Parameters

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



CHAPTER 4

Configuring RADIUS

This chapter contains the following sections:

- [Configuring RADIUS, on page 19](#)

Configuring RADIUS

Information About RADIUS

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

RADIUS Network Environments

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

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

- Networks with multiple-vendor network devices, each supporting RADIUS.

For example, network devices from several vendors can use a single RADIUS server-based security database.

- Networks already using RADIUS.

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

- Networks that require resource accounting.

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

- Networks that support authentication profiles.

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

Information About RADIUS Operations

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

1. The user is prompted for and enters a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of the following responses from the RADIUS server:
 - ACCEPT—The user is authenticated.
 - REJECT—The user is not authenticated and is prompted to reenter the username and password, or access is denied.
 - CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.
 - CHANGE PASSWORD—A request is issued by the RADIUS server, asking the user to select a new password.

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

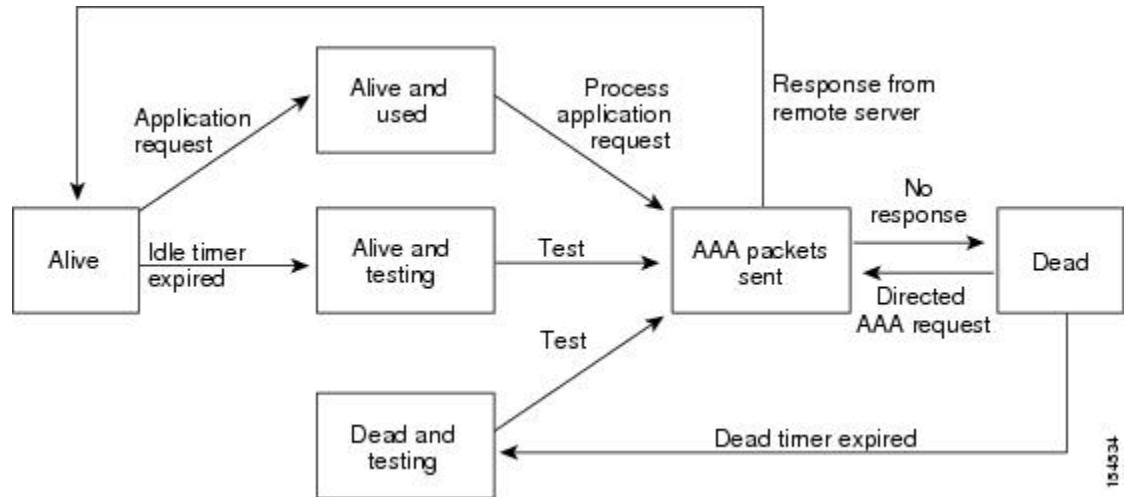
- Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IPv4 address, access list, and user timeouts.

RADIUS Server Monitoring

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

The following figure shows the different RADIUS server states:

Figure 2: RADIUS Server States



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.

Vendor-Specific Attributes

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

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

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

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

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

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

The Cisco Nexus device supports the following attributes:

- roles—Lists all the roles to which the user belongs. The value field is a string that lists the role names delimited by white spaces.

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

Prerequisites for RADIUS

RADIUS has the following prerequisites:

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

Guidelines and Limitations for RADIUS

RADIUS has the following configuration guidelines and limitations:

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

Configuring RADIUS Servers

This section describes how to configure RADIUS servers.

Procedure

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

Configuring RADIUS Server Hosts

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

Procedure

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

Example

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

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

Configuring RADIUS Global Preshared Keys

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

Before you begin

Obtain the preshared key values for the remote RADIUS servers

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# radius-server key [0 7] <i>key-value</i>	Specifies a preshared key for all RADIUS servers. You can specify a clear text (0) or encrypted (7) preshared key. The default format is clear text. The maximum length is 63 characters.

	Command or Action	Purpose
		By default, no preshared key is configured.
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	(Optional) switch# show radius-server	Displays the RADIUS server configuration. Note The preshared keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted preshared keys.
Step 5	(Optional) switch# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure preshared keys at the global level for all servers used by the device:

```
switch# configure terminal
switch(config)# radius-server key 0 QsEfThUkO
switch(config)# exit
switch# copy running-config startup-config
```

Configuring RADIUS Server Preshared Keys

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

Before you begin

Obtain the preshared key values for the remote RADIUS servers.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# radius-server host { <i>ipv4-address</i> <i>host-name</i> } key [0 7] <i>key-value</i>	Specifies a preshared key for a specific RADIUS server. You can specify a clear text (0) or encrypted (7) preshared key. The default format is clear text. The maximum length is 63 characters. This preshared key is used instead of the global preshared key.
Step 3	switch(config)# exit	Exits configuration mode.

	Command or Action	Purpose
Step 4	(Optional) switch# show radius-server	Displays the RADIUS server configuration. Note The preshared keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted preshared keys.
Step 5	(Optional) switch# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure RADIUS preshared keys:

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

Configuring RADIUS Server Groups

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch (config)# aaa group server radius <i>group-name</i>	Creates a RADIUS server group and enters the RADIUS server group configuration submode for that group. The <i>group-name</i> argument is a case-sensitive, alphanumeric string with a maximum of 127 characters.
Step 3	switch (config-radius)# server { <i>ipv4-address</i> <i> server-name</i> }	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.

	Command or Action	Purpose
Step 4	(Optional) switch (config-radius)# deadtime <i>minutes</i>	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) switch(config-radius)# source-interface <i>interface</i>	Assigns a source interface for a specific RADIUS server group. The supported interface types are management and VLAN. Note Use the source-interface command to override the global source interface assigned by the ip radius source-interface command.
Step 6	switch(config-radius)# exit	Exits configuration mode.
Step 7	(Optional) switch(config)# show radius-server group [<i>group-name</i>]	Displays the RADIUS server group configuration.
Step 8	(Optional) switch(config)# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

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

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

What to do next

Apply the RADIUS server groups to an AAA service.

Configuring the Global Source Interface for RADIUS Server Groups

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# ip radius source-interface interface	Configures the global source interface for all RADIUS server groups configured on the device. The source interface can be the management or the VLAN interface.
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	(Optional) switch# show radius-server	Displays the RADIUS server configuration information.
Step 5	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

This example shows how to configure the mgmt 0 interface as the global source interface for RADIUS server groups:

```
switch# configure terminal
switch(config)# ip radius source-interface mgmt 0
switch(config)# exit
switch# copy running-config startup-config
```

Allowing Users to Specify a RADIUS Server at Login

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	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	switch(config)# exit	Exits configuration mode.
Step 4	(Optional) switch# show radius-server directed-request	Displays the directed request configuration.
Step 5	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

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

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

Configuring the Global RADIUS Transmission Retry Count and Timeout Interval

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# radius-server retransmit <i>count</i>	Specifies the retransmission count for all RADIUS servers. The default retransmission count is 1 and the range is from 0 to 5.
Step 3	switch(config)# radius-server timeout <i>seconds</i>	Specifies the transmission timeout interval for RADIUS servers. The default timeout interval is 5 seconds and the range is from 1 to 60 seconds.
Step 4	switch(config)# exit	Exits global configuration mode.
Step 5	(Optional) switch# show radius-server	Displays the RADIUS server configuration.
Step 6	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

This example shows how to set the retry count to 3 and the transmission timeout interval to 5 seconds for RADIUS servers:

```
switch# configure terminal
switch(config)# radius-server retransmit 3
switch(config)# radius-server timeout 5
switch(config)# exit
switch# copy running-config startup-config
```


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

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# radius-server host <i>{ipv4-address host-name}</i> retransmit count	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	switch(config)# radius-server host <i>{ipv4-address host-name}</i> timeout seconds	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	switch(config)# exit	Exits global configuration mode.
Step 5	(Optional) switch# show radius-server	Displays the RADIUS server configuration.
Step 6	(Optional) switch# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

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

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

Configuring Accounting and Authentication Attributes for RADIUS Servers

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	(Optional) switch(config)# radius-server host { <i>ipv4-address</i> <i>host-name</i> } acct-port <i>udp-port</i>	Specifies a UDP port to use for RADIUS accounting messages. The default UDP port is 1812. The range is from 0 to 65535.
Step 3	(Optional) switch(config)# radius-server host { <i>ipv4-address</i> <i>host-name</i> } accounting	Specifies that the specified RADIUS server is to be used only for accounting purposes. The default is both accounting and authentication.
Step 4	(Optional) switch(config)# radius-server host { <i>ipv4-address</i> <i>host-name</i> } auth-port <i>udp-port</i>	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) switch(config)# radius-server host { <i>ipv4-address</i> <i>host-name</i> } authentication	Specifies that the specified RADIUS server only be used for authentication purposes. The default is both accounting and authentication.
Step 6	switch(config)# exit	Exits configuration mode.
Step 7	(Optional) switch(config)# show radius-server	Displays the RADIUS server configuration.
Step 8	switch(config)# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

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

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

Configuring Periodic RADIUS Server Monitoring

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



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

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

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# radius-server host { <i>ipv4-address</i> <i>host-name</i> } test { idle-time <i>minutes</i> password <i>password</i> [idle-time <i>minutes</i>] username <i>name</i> [password <i>password</i> [idle-time <i>minutes</i>]]}	Specifies parameters for server monitoring. The default username is test and the default password is test. The default value for the idle timer is 0 minutes. 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	switch(config)# radius-server deadtime <i>minutes</i>	Specifies the number of minutes before the switch checks a RADIUS server that was previously unresponsive. The default value is 0 minutes. The valid range is 1 to 1440 minutes.
Step 4	switch(config)# exit	Exits configuration mode.
Step 5	(Optional) switch# show radius-server	Displays the RADIUS server configuration.
Step 6	(Optional) switch# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

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

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

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

Configuring the Dead-Time Interval

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



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.

Procedure

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

Example

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

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

Manually Monitoring RADIUS Servers or Groups

Procedure

	Command or Action	Purpose
Step 1	switch# test aaa server radius <i>{ipv4-address server-name}</i> [vrf <i>vrf-name</i>] <i>username password</i> test aaa server radius <i>{ipv4-address server-name}</i> [vrf <i>vrf-name</i>] <i>username password</i>	Sends a test message to a RADIUS server to confirm availability.

	Command or Action	Purpose
Step 2	switch# test aaa group <i>group-name username password</i>	Sends a test message to a RADIUS server group to confirm availability.

Example

This example shows how to send a test message to the RADIUS server and server group to confirm availability:

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

Verifying the RADIUS Configuration

Displaying RADIUS Server Statistics

Procedure

	Command or Action	Purpose
Step 1	switch# show radius-server statistics <i>{hostname ipv4-address}</i>	Displays the RADIUS statistics.

Clearing RADIUS Server Statistics

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

Before you begin

Configure RADIUS servers on the Cisco NX-OS device.

Procedure

	Command or Action	Purpose
Step 1	(Optional) switch# show radius-server statistics <i>{hostname ipv4-address}</i>	Displays the RADIUS server statistics on the Cisco NX-OS device.
Step 2	switch# clear radius-server statistics <i>{hostname ipv4-address}</i>	Clears the RADIUS server statistics.

Configuration Examples for RADIUS

The following example shows how to configure RADIUS:

```
switch# configure terminal
```

```

switch(config)# radius-server key 7 "ToIkLhPpG"
switch(config)# radius-server host 10.10.1.1 key 7 "ShMoMhT1" authentication accounting
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
switch(config-radius)# exit
switch(config-radius)# use-vrf management

```

Default Settings for RADIUS

The following table lists the default settings for RADIUS parameters.

Table 6: Default RADIUS Parameters

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



CHAPTER 5

Configuring TACACS+

This chapter contains the following sections:

- [About Configuring TACACS+, on page 35](#)

About Configuring TACACS+

Information About Configuring TACACS+

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

TACACS+ provides for separate authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service (authentication, authorization, and accounting) independently. Each service is associated with its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The TACACS+ client/server protocol uses TCP (TCP port 49) for transport requirements. The Cisco Nexus device provides centralized authentication using the TACACS+ protocol.

TACACS+ Advantages

TACACS+ has the following advantages over RADIUS authentication:

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

User Login with TACACS+

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

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



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 the user's mother's maiden name.

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

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

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

Services include the following:

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

Default TACACS+ Server Encryption Type and Preshared Key

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

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

Command Authorization Support for TACACS+ Servers

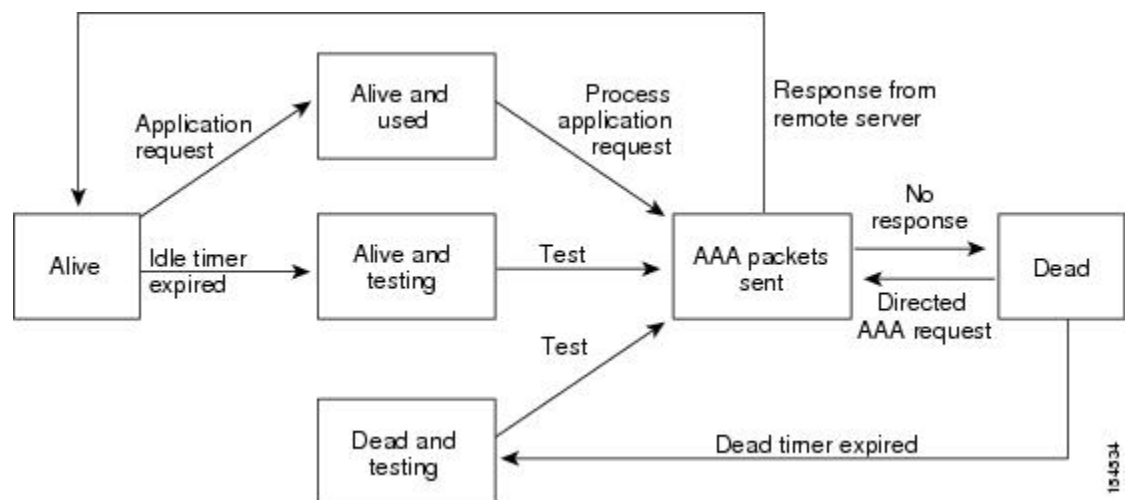
By default, command authorization is done against a local database in the Cisco NX-OS software when an authenticated user enters a command at the command-line interface (CLI). You can also verify authorized commands for authenticated users using TACACS+.

TACACS+ Server Monitoring

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

The following figure shows the different TACACS+ server states:

Figure 3: TACACS+ Server States



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

Prerequisites for TACACS+

TACACS+ has the following prerequisites:

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

Guidelines and Limitations for TACACS+

TACACS+ has the following configuration guidelines and limitations:

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

Configuring TACACS+

TACACS+ Server Configuration Process

This section describes how to configure TACACS+ servers.

Procedure

-
- Step 1** Enable TACACS+.
- Step 2** Establish the TACACS+ server connections to the Cisco Nexus device.
- Step 3** Configure the preshared secret keys for the TACACS+ servers.
- Step 4** If needed, configure TACACS+ server groups with subsets of the TACACS+ servers for AAA authentication methods.
- Step 5** If needed, configure any of the following optional parameters:
- Dead-time interval
 - Allow TACACS+ server specification at login
 - Timeout interval
 - TCP port
- Step 6** If needed, configure periodic TACACS+ server monitoring.
-

Enabling TACACS+

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# feature tacacs+	Enables TACACS+.
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	(Optional) 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 IPv4 address or the hostname for the TACACS+ server on the Cisco Nexus device. All TACACS+ server hosts are added to the default TACACS+ server group. You can configure up to 64 TACACS+ servers.

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

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

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# tacacs-server host { <i>ipv4-address</i> <i>host-name</i> }	Specifies the IPv4 address or hostname for a TACACS+ server.
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	(Optional) switch# show tacacs-server	Displays the TACACS+ server configuration.
Step 5	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

You can delete a TACACS+ server host from a server group.

Configuring TACACS+ Global Preshared Keys

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

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

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	tacacs-server key [0 6 7] <i>key-value</i>	Specifies a TACACS+ key for all TACACS+ server. You can specify that the <i>key-value</i> is in clear text format (0), is type-6 encrypted (6), or

	Command or Action	Purpose
		is type-7 encrypted (7). The default format is clear text. The maximum length is 63 characters. By default, no preshared key is configured.
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	(Optional) switch# show tacacs-server	Displays the TACACS+ server configuration. Note The preshared keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted preshared keys.
Step 5	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

The following example shows how to configure global preshared keys:

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

Configuring TACACS+ Server Preshared Keys

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# tacacs-server host <i>{ipv4-address host-name} key [0 7]</i> <i>key-value</i>	Specifies a preshared key for a specific TACACS+ server. You can specify a clear text (0) or encrypted (7) preshared key. The default format is clear text. The maximum length is 63 characters. This preshared key is used instead of the global preshared key.
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	(Optional) switch# show tacacs-server	Displays the TACACS+ server configuration.

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

Example

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

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

Configuring TACACS+ Server Groups

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

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

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# aaa group server tacacs+ group-name	Creates a TACACS+ server group and enters the TACACS+ server group configuration mode for that group.
Step 3	switch(config)# tacacs-server host {ipv4-address host-name} key [0 7] key-value	Specifies a preshared key for a specific TACACS+ server. You can specify a clear text (0) or encrypted (7) preshared key. The default format is clear text. The maximum length is 63 characters. This preshared key is used instead of the global preshared key.

	Command or Action	Purpose
Step 4	(Optional) switch(config-tacacs+)# deadtime <i>minutes</i>	Configures the monitoring dead time. The default is 0 minutes. The range is from 0 through 1440. Note If the dead-time interval for a TACACS+ server group is greater than zero (0), that value takes precedence over the global dead-time value.
Step 5	(Optional) switch(config-tacacs+)# source-interface <i>interface</i>	Assigns a source interface for a specific TACACS+ server group. The supported interface types are management and VLAN. Note Use the source-interface command to override the global source interface assigned by the ip tacacs source-interface command.
Step 6	switch(config-tacacs+)# exit	Exits configuration mode.
Step 7	(Optional) switch(config)# show tacacs-server groups	Displays the TACACS+ server group configuration.
Step 8	(Optional) switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

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

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
switch(config-tacacs+)# deadtime 30
switch(config-tacacs+)# exit
switch(config)# show tacacs-server groups
switch(config)# copy running-config startup-config
```

Configuring the Global Source Interface for TACACS+ Server Groups

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

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	ip tacacs source-interface <i>interface</i> Example: switch(config)# ip tacacs source-interface mgmt 0	Configures the global source interface for all TACACS+ server groups configured on the device. The source interface can be the management or the VLAN interface.
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.

Specifying a TACACS+ Server at Login

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



Note User specified logins are only supported for Telnet sessions.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	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	switch(config)# exit	Exits configuration mode.
Step 4	(Optional) switch# show tacacs-server directed-request	Displays the TACACS+ directed request configuration.

	Command or Action	Purpose
Step 5	(Optional) <code>switch# copy running-config startup-config</code>	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+.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	aaa authorization ssh-certificate default {group group-list [none] local none} Example: <pre>switch(config)# aaa authorization ssh-certificate default group TACACSServer1 TACACSServer2</pre>	<p>Configures the default AAA authorization method for the TACACS+ servers.</p> <p>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.</p> <p>The <i>group-list</i> 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.</p>
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 4	(Optional) show aaa authorization [all] Example: <pre>switch# show aaa authorization</pre>	Displays the AAA authorization configuration. The all keyword displays the default values.
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	

Configuring Command Authorization on TACACS+ Servers

You can configure authorization for commands on TACACS+ servers. Command authorization disables user role-based authorization control (RBAC), including the default roles.

Before you begin

Enable TACACS+.

Configure TACACS host and server groups before configuring AAA command authorization.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	aaa authorization {commands config-commands} default [group group-list [local] local] Example: <pre>switch(config)# aaa authorization commands default group TacGroup</pre>	<p>Configures the default authorization method for commands for all roles.</p> <p>The commands keyword configures authorization sources for all EXEC commands, and the config-commands keyword configures authorization sources for all configuration commands. The default authorization for all commands is local authorization, which is the list of authorized commands for the user's assigned role.</p> <p>The <i>group-list</i> argument consists of a space-delimited list of TACACS+ server group names. Servers that belong to this group are contacted for command authorization. The local method uses the local role-based database for authorization.</p> <p>The local method is used only if all the configured server groups fail to respond and you have configured local as the fallback method.</p> <p>The default method is local.</p> <p>If you have not configured a fallback method after the TACACS+ server group method, authorization fails if all server groups fail to respond.</p>

	Command or Action	Purpose
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 4	(Optional) show aaa authorization [all] Example: <pre>switch(config)# show aaa authorization</pre>	Displays the AAA authorization configuration. The all keyword displays the default values.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

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 the results might not be reliable.

Before you begin

Enable TACACS+.

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

Procedure

	Command or Action	Purpose
Step 1	test aaa authorization command-type {commands config-commands} user username command command-string Example: <pre>switch# test aaa authorization command-type commands user TestUser command reload</pre>	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 <i>command-string</i> argument if it contains spaces.

Enabling and Disabling Command Authorization Verification

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



Note The commands do not execute when you enable authorization verification.

Procedure

	Command or Action	Purpose
Step 1	terminal verify-only [<i>username username</i>] 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 [<i>username username</i>] 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
13 - 1	<ul style="list-style-type: none"> 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).

Procedure

	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 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 <i>password</i> argument can be up to 64 alphanumeric characters. The <i>priv-lvl</i> 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.
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 <i>level</i> argument specifies the

	Command or Action	Purpose
		privilege level to which the user is granted access. The only available level is 15.

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**.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no] role name priv-<i>n</i> Example: <pre>switch(config)# role name priv-5 switch(config-role)#</pre>	Enables or disables a privilege role and enters role configuration mode. The <i>n</i> argument specifies the privilege level and is a number between 0 and 13.
Step 3	rule <i>number</i> {deny permit} command <i>command-string</i> Example: <pre>switch(config-role)# rule 2 permit command pwd</pre>	<p>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.</p> <p>The <i>command-string</i> argument can contain spaces.</p> <p>Note Repeat this command for 256 rules.</p>
Step 4	exit Example: <pre>switch(config-role)# exit switch(config)#</pre>	Exits role configuration mode.

	Command or Action	Purpose
Step 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Configuring the Global TACACS+ Timeout Interval

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

Procedure

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

Configuring the Timeout Interval for a Server

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# switch(config)# tacacs-server host {ipv4-address host-name} timeout seconds	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	switch(config)# exit	Exits configuration mode.

	Command or Action	Purpose
Step 4	(Optional) switch# show tacacs-server	Displays the TACACS+ server configuration.
Step 5	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Configuring TCP Ports

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# tacacs-server host <i>{ipv4-address host-name}</i> port tcp-port	Specifies the UDP port to use for TACACS+ accounting messages. The default TCP port is 49. The range is from 1 to 65535.
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	(Optional) switch# show tacacs-server	Displays the TACACS+ server configuration.
Step 5	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

The following example shows how to configure TCP ports:

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

Configuring Periodic TACACS+ Server Monitoring

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



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

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



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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# tacacs-server host { <i>ipv4-address</i> <i>host-name</i> } test { idle-time <i>minutes</i> password <i>password</i> [idle-time <i>minutes</i>] username <i>name</i> [password <i>password</i> [idle-time <i>minutes</i>]]}	Specifies parameters for 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	switch(config)# tacacs-server dead-time <i>minutes</i>	Specifies the number minutes before the Cisco Nexus device checks a TACACS+ server that was previously unresponsive. The default value is 0 minutes and the valid range is 0 to 1440 minutes.
Step 4	switch(config)# exit	Exits configuration mode.
Step 5	(Optional) switch# show tacacs-server	Displays the TACACS+ server configuration.
Step 6	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

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

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


Configuring the Dead-Time Interval

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



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

Procedure

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

Manually Monitoring TACACS+ Servers or Groups

Procedure

	Command or Action	Purpose
Step 1	switch# test aaa server tacacs+ <i>{ipv4-address host-name}</i> [<i>vrf vrf-name</i>] <i>username password</i>	Sends a test message to a TACACS+ server to confirm availability.
Step 2	switch# test aaa group <i>group-name username password</i>	Sends a test message to a TACACS+ server group to confirm availability.

Example

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

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

Disabling TACACS+

You can disable TACACS+.

**Caution**

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# no feature tacacs+	Disables TACACS+.
Step 3	switch(config)# exit	Exits configuration mode.
Step 4	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Displaying TACACS+ Statistics

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

Procedure

	Command or Action	Purpose
Step 1	switch# show tacacs-server statistics {hostname ipv4-address}	Displays the TACACS+ statistics.

Example

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

Verifying the TACACS+ Configuration

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

Procedure

	Command or Action	Purpose
Step 1	switch# show tacacs+ {status pending pending-diff}	Displays the TACACS+ Cisco Fabric Services distribution status and other details.
Step 2	switch# show running-config tacacs [all]	Displays the TACACS+ configuration in the running configuration.
Step 3	switch# show startup-config tacacs	Displays the TACACS+ configuration in the startup configuration.

	Command or Action	Purpose
Step 4	switch# show tacacs-serve [<i>host-name</i> <i>ipv4-address</i>] [<i>directed-request</i> groups sorted statistics]	Displays all configured TACACS+ server parameters.

Configuration Examples for TACACS+

This example shows how to configure TACACS+:

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

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

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

switch(config)# aaa group server tacacs+ TacServer1
switch(config-tacacs+)# server 1.1.1.1
switch(config-tacacs+)# server 1.1.1.2
```

Default Settings for TACACS+

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

Table 7: Default TACACS+ Parameters

Parameters	Default
TACACS+	Disabled
Dead-time interval	0 minutes
Timeout interval	5 seconds
Idle timer interval	0 minutes
Periodic server monitoring username	test
Periodic server monitoring password	test



CHAPTER 6

Configuring SSH and Telnet

This chapter contains the following sections:

- [Configuring SSH and Telnet, on page 57](#)

Configuring SSH and Telnet

Information About SSH and Telnet

SSH Server

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

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

SSH Client

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

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

SSH Server Keys

SSH requires server keys for secure communications to the Cisco Nexus device. You can use SSH keys for the following SSH options:

- SSH version 2 using Rivest, Shamir, and Adelman (RSA) public-key cryptography
- SSH version 2 using the Digital System Algorithm (DSA)

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

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

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

SSH supports the following public key formats:

- OpenSSH
- IETF Secure Shell (SECSH)


Caution

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

Telnet Server

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

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

Guidelines and Limitations for SSH

SSH has the following configuration guidelines and limitations:

- The Cisco Nexus device supports only SSH version 2 (SSHv2).

Configuring 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.

Procedure

	Command or Action	Purpose
Step 1	<code>switch# configure terminal</code>	Enters global configuration mode.
Step 2	<code>switch(config)# ssh key {dsa [force] rsa [bits] [force]}</code>	Generates the SSH server key. The <i>bits</i> argument is the number of bits used to generate the key. The range is from 768 to 2048 and the default value is 1024.

	Command or Action	Purpose
		Use the force keyword to replace an existing key.
Step 3	switch(config)# exit	Exits global configuration mode.
Step 4	(Optional) switch# show ssh key	Displays the SSH server keys.
Step 5	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

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

```
switch# configure terminal
switch(config)# ssh key rsa 2048
switch(config)# exit
switch# show ssh key
switch# copy running-config startup-config
```

Specifying the SSH Public Keys for User Accounts

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

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

Specifying the SSH Public Keys in Open SSH Format

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

Procedure

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

Example

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

```
switch# configure terminal
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```



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

Specifying the SSH Public Keys in IETF SECSH Format

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

Procedure

	Command or Action	Purpose
Step 1	switch# <code>copy server-file bootflash: filename</code>	Downloads the file that contains the SSH key in IETF SECSH format from a server. The server can be FTP, SCP, SFTP, or TFTP.
Step 2	switch# <code>configure terminal</code>	Enters global configuration mode.
Step 3	switch(config)# <code>username username sshkey file filename</code>	Configures the SSH public key in SSH format.
Step 4	switch(config)# <code>exit</code>	Exits global configuration mode.
Step 5	(Optional) switch# <code>show user-account</code>	Displays the user account configuration.
Step 6	(Optional) switch# <code>copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Example

The following example shows how to specify the SSH public key in the IETF SECSH format:

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


Specifying the SSH Public Keys in PEM-Formatted Public Key Certificate Form

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

Procedure

	Command or Action	Purpose
Step 1	switch# <code>copy server-file bootflash: filename</code>	Downloads the file that contains the SSH key in PEM-formatted Public Key Certificate form from a server. The server can be FTP, SCP, SFTP, or TFTP
Step 2	switch# <code>configure terminal</code>	Enters global configuration mode.
Step 3	(Optional) switch# <code>show user-account</code>	Displays the user account configuration.
Step 4	(Optional) switch# <code>copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Example

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

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

Starting SSH Sessions to Remote Devices

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

Procedure

	Command or Action	Purpose
Step 1	switch# <code>ssh {hostname username@hostname} [vrf vrf-name]</code>	Creates an SSH session to a remote device. The <i>hostname</i> argument can be an IPv4 address or a hostname.

Clearing SSH Hosts

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

Procedure

	Command or Action	Purpose
Step 1	switch# <code>clear ssh hosts</code>	Clears the SSH host sessions.

Disabling the SSH Server

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# [no] feature ssh	Enables/disables the SSH server. The default is enabled.
Step 3	switch(config)# exit	Exits global configuration mode.
Step 4	(Optional) switch# show ssh server	Displays the SSH server configuration.
Step 5	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Deleting SSH Server Keys

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



Note To reenble SSH, you must first generate an SSH server key.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# no feature ssh	Disables the SSH server.
Step 3	switch(config)# no ssh key [dsa rsa]	Deletes the SSH server key. The default is to delete all the SSH keys.
Step 4	switch(config)# exit	Exits global configuration mode.
Step 5	(Optional) switch# show ssh key	Displays the SSH server configuration.
Step 6	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Clearing SSH Sessions

You can clear SSH sessions from the Cisco Nexus device.

Procedure

	Command or Action	Purpose
Step 1	switch# show users	Displays user session information.
Step 2	switch# clear line vty-line	Clears a user SSH session.

Configuration Examples for SSH

The following example shows how to configure SSH:

Procedure**Step 1**

Generate an SSH server key.

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

Step 2

Enable the SSH server.

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

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

Step 3

Display the SSH server key.

```
switch(config)# show ssh key
rsa Keys generated:Fri May 8 22:09:47 2009

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAEARI3mQy4W1AV9Y2t2hrEWgbUEYzCfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZ/
cTFEzaAAZp9AS86dgBAjsKGs7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4ZXIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5/
Ninn0Mc=

bitcount:1024
fingerprint:
4b:4d:f6:b9:42:e9:d9:71:3c:bd:09:94:4a:93:ac:ca
*****
could not retrieve dsa key information
*****
```

Step 4

Specify the SSH public key in Open SSH format.

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CfTP05B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
```

Step 5 Save the configuration.

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

Configuring Telnet

Enabling the Telnet Server

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

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# [no] feature telnet	Enables/disables the Telnet server. The default is enabled.

Reenabling the Telnet Server

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

Procedure

	Command or Action	Purpose
Step 1	switch(config)# [no] feature telnet	Reenables the Telnet server.

Starting Telnet Sessions to Remote Devices

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

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

Procedure

	Command or Action	Purpose
Step 1	switch# telnet <i>hostname</i>	Creates a Telnet session to a remote device. The <i>hostname</i> argument can be an IPv4 address or a device name.

Example

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

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

Clearing Telnet Sessions

You can clear Telnet sessions from the Cisco Nexus device.

Procedure

	Command or Action	Purpose
Step 1	switch# show users	Displays user session information.
Step 2	switch# clear line <i>vtty-line</i>	Clears a user Telnet session.

Verifying the SSH and Telnet Configuration

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

Procedure

- switch# **show ssh key** [*dsa* | *rsa*]

Command or Action	Purpose
switch# show running-config security [<i>all</i>]	Displays the SSH and user account configuration in the running configuration. The all keyword displays the default values for the SSH and user accounts.
switch# show ssh server	Displays the SSH server configuration.
switch# show user-account	Displays user account information

Default Settings for SSH

The following table lists the default settings for SSH parameters.

Table 8: Default SSH Parameters

Parameters	Default
SSH server	Enabled
SSH server key	RSA key generated with 1024 bits
RSA key bits for generation	1024
Telnet server	Enabled



CHAPTER 7

Configuring Access Control Lists

This chapter contains the following sections:

- [Information About ACLs, on page 67](#)
- [Configuring IP ACLs, on page 74](#)
- [Information About VLAN ACLs, on page 80](#)
- [Configuring VACLs, on page 81](#)
- [Configuration Examples for VACL, on page 83](#)
- [Configuring ACL TCAM Region Sizes, on page 83](#)
- [Configuring ACLs on Virtual Terminal Lines, on page 86](#)

Information About ACLs

An access control list (ACL) is an ordered set of rules that you can use to filter traffic. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When the switch determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether the packet is permitted or denied. If there is no match, the switch applies the applicable default rule. The switch continues processing packets that are permitted and drops packets that are denied.

You can use ACLs to protect networks and specific hosts from unnecessary or unwanted traffic. For example, you could use ACLs to disallow HTTP traffic from a high-security network to the Internet. You could also use ACLs to allow HTTP traffic but only to specific sites, using the IP address of the site to identify it in an IP ACL.

IP ACL Types and Applications

The Cisco Nexus device supports IPv4 for security traffic filtering. The switch allows you to use IP access control lists (ACLs) as port ACLs, VLAN ACLs, and Router ACLs as shown in the following table.

Table 9: Security ACL Applications

Application	Supported Interfaces	Types of ACLs Supported
Port ACL	<p>An ACL is considered a port ACL when you apply it to one of the following:</p> <ul style="list-style-type: none"> • Ethernet interface • Ethernet port-channel interface <p>When a port ACL is applied to a trunk port, the ACL filters traffic on all VLANs on the trunk port.</p>	IPv4 ACLs
Router ACL	<ul style="list-style-type: none"> • VLAN interfaces <p>Note You must enable VLAN interfaces globally before you can configure a VLAN interface.</p> <ul style="list-style-type: none"> • Physical Layer 3 interfaces • Layer 3 Ethernet subinterfaces • Layer 3 Ethernet port-channel interfaces • Layer 3 Ethernet port-channel subinterfaces • Tunnels • Management interfaces 	IPv4 ACLs
VLAN ACL (VACL)	<p>An ACL is a VACL when you use an access map to associate the ACL with an action and then apply the map to a VLAN.</p>	IPv4 ACLs
VTY ACL	VTYs	IPv4 ACLs

Application Order

When the device processes a packet, it determines the forwarding path of the packet. The path determines which ACLs that the device applies to the traffic. The device applies the ACLs in the following order:

1. Port ACL
2. Ingress VACL
3. Ingress Router ACL
4. Egress Router ACL
5. Egress VACL

Rules

Rules are what you create, modify, and remove when you configure how an ACL filters network traffic. Rules appear in the running configuration. When you apply an ACL to an interface or change a rule within an ACL that is already applied to an interface, the supervisor module creates ACL entries from the rules in the running configuration and sends those ACL entries to the applicable I/O module. Depending upon how you configure the ACL, there may be more ACL entries than rules, especially if you implement policy-based ACLs by using object groups when you configure rules.

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.

Source and Destination

In each rule, you specify the source and the destination of the traffic that matches the rule. You can specify both the source and destination as a specific host, a network or group of hosts, or any host.

Protocols

IPv4 and MAC ACLs allow you to identify traffic by protocol. For your convenience, you can specify some protocols by name. For example, in an IPv4 ACL, you can specify ICMP by name.

You can specify any protocol by the integer that represents the Internet protocol number.

Implicit Rules

IP and MAC ACLs have implicit rules, which means that although these rules do not appear in the running configuration, the switch applies them to traffic when no other rules in an ACL match.

All IPv4 ACLs include the following implicit rule:

```
deny ip any any
```

This implicit rule ensures that the switch denies unmatched IP traffic.

```
permit icmp any any nd-na
permit icmp any any nd-ns
permit icmp any any router-advertisement
permit icmp any any router-solicitation
```

All MAC ACLs include the following implicit rule:

```
deny any any protocol
```

This implicit rule ensures that the device denies the unmatched traffic, regardless of the protocol specified in the Layer 2 header of the traffic.

Additional Filtering Options

You can identify traffic by using additional options. IPv4 ACLs support the following additional filtering options:

- Layer 4 protocol
- TCP and UDP ports

- ICMP types and codes
- IGMP types
- Precedence level
- Differentiated Services Code Point (DSCP) value
- TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
- Established TCP connections

Sequence Numbers

The Cisco Nexus device supports sequence numbers for rules. Every rule that you enter receives a sequence number, either assigned by you or assigned automatically by the device. Sequence numbers simplify the following ACL tasks:

- Adding new rules between existing rules—By specifying the sequence number, you specify where in the ACL a new rule should be positioned. For example, if you need to insert a rule between rules numbered 100 and 110, you could assign a sequence number of 105 to the new rule.
- Removing a rule—Without using a sequence number, removing a rule requires that you enter the whole rule, as follows:

```
switch(config-acl)# no permit tcp 10.0.0.0/8 any
```

However, if the same rule had a sequence number of 101, removing the rule requires only the following command:

```
switch(config-acl)# no 101
```

- Moving a rule—With sequence numbers, if you need to move a rule to a different position within an ACL, you can add a second instance of the rule using the sequence number that positions it correctly, and then you can remove the original instance of the rule. This action allows you to move the rule without disrupting traffic.

If you enter a rule without a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule to the rule. For example, if the last rule in an ACL has a sequence number of 225 and you add a rule without a sequence number, the device assigns the sequence number 235 to the new rule.

In addition, the device allows you to reassign sequence numbers to rules in an ACL. 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 Cisco Nexus device stores operator-operand couples in registers called logical operation units (LOUs) to perform operations (greater than, less than, not equal to, and range) on the TCP and UDP ports specified in an IP ACL.



Note The range operator is inclusive of boundary values.

These LOUs minimize the number of ternary content addressable memory (TCAM) entries needed to perform these operations. A maximum of two LOUs are allowed for each feature on an interface. For example an ingress RACL can use two LOUs, and a QoS feature can use two LOUs. If an ACL feature requires more than two arithmetic operations, the first two operations use LOUs, and the remaining access control entries (ACEs) get expanded.

The following guidelines determine when the device stores operator-operand couples in LOUs:

- If the operator or operand differs from other operator-operand couples that are used in other rules, the couple is stored in an LOU.

For example, the operator-operand couples "gt 10" and "gt 11" would be stored separately in half an LOU each. The couples "gt 10" and "lt 10" would also be stored separately.

- Whether the operator-operand couple is applied to a source port or a destination port in the rule affects LOU usage. Identical couples are stored separately when one of the identical couples is applied to a source port and the other couple is applied to a destination port.

For example, if a rule applies the operator-operand couple "gt 10" to a source port and another rule applies a "gt 10" couple to a destination port, both couples would also be stored in half an LOU, resulting in the use of one whole LOU. Any additional rules using a "gt 10" couple would not result in further LOU usage.

ACL TCAM Regions

You can change the size of the ACL ternary content addressable memory (TCAM) regions in the hardware.

The IPv4 TCAMs are single wide.

TCAM region sizes have the following guidelines and limitations:

- To revert to the default ACL TCAM size, use the **no hardware profile tcam region** command. You no longer need to use the **write erase command** and reload the switch.
- Depending on the Cisco Nexus device, each TCAM region might have a different minimum/maximum/aggregate size restriction.
- The default size of the ARPACL TCAM is zero. Before you use the ARP ACLs in a Control Policing Plane (CoPP) policy, you must set the size of this TCAM to a non-zero size.
- You must set the VACL and egress VLAN ACL (E-VACL) size to the same value.
- The total TCAM depth is 2000 for ingress and 1000 for egress, which can be carved in 256 entries blocks.
- After TCAM carving, you must reload the switch.
- All existing TCAMs cannot be set to size 0.
- By default, all IPv6 TCAMs are disabled (the TCAM size is set to 0).

Table 10: TCAM Sizes by ACL Region

TCAM ACL Region	Default Size	Minimum Size	Incremental Size
SUP (ingress)	112	48	16
PACL (ingress)	400	0	16

TCAM ACL Region	Default Size	Minimum Size	Incremental Size
VACL (ingress), VACL (egress)	640 (ingress), 640 (egress)	0 (ingress), 0 (egress)	16
RACL (ingress)	1536	0	16
QOS (ingress), QOS (egress)	192 (ingress), 64 (egress)	16 (ingress), 64 (egress)	16
E-VACL (egress)	640	0	16
E-RACL (egress)	256	0	16
NAT	256	0	16

Licensing Requirements for ACLs

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	No license is required to use ACLs.

Prerequisites for ACLs

IP ACLs have the following prerequisites:

- You must be familiar with IP addressing and protocols to configure IP ACLs.
- You must be familiar with the interface types that you want to configure with ACLs.

VACLs have the following prerequisite:

- Ensure that the IP ACL that you want to use in the VACL exists and is configured to filter traffic in the manner that you need for this application.

Guidelines and Limitations for ACLs

IP ACLs have the following configuration guidelines and limitations:

- We recommend that you perform ACL configuration using the Session Manager. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. This is especially useful for ACLs that include more than about 1000 rules.
- 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).

- To apply an IP ACL to a VLAN interface, you must have enabled VLAN interfaces globally.
- One VLAN access map can match only one IP ACL.
- An IP ACL can have multiple permit/deny ACEs.
- One VLAN can have only one access map applied.
- Egress RACLs and VACLs should not be applied in warp mode, and it is not supported.
- Egress ACLs cannot be applied to multicast traffic.
- Although Ingress RACLs on SVI are supported for multicast traffic, if the ACL defining the multicast group where the traffic needs to be sent to or sourced from includes the **log** keyword, the ingress RACL application on SVI is not supported.
- PACL cannot be applied in warp mode.
- The same ingress RACL on an SVI and on a Layer 3 interface cannot share TCAM resources, and they individually use up TCAM resources. However, they share ACL statistics resources. If the RACL TCAM is almost depleted before upgrade, RACL application may fail after upgrade. If this happens, you can carve the RACL TCAM.
- ARP ACLs are not supported on the Nexus 3500 platform.

Default ACL Settings

The following table lists the default settings for IP ACLs parameters.

Table 11: Default IP ACLs Parameters

Parameters	Default
IP ACLs	No IP ACLs exist by default.
ACL rules	Implicit rules apply to all ACLs .
Object groups	No object groups exist by default.

The following table lists the default settings for VACL parameters.

Table 12: Default VACL Parameters

Parameters	Default
VACLs	No IP ACLs exist by default.
ACL rules	Implicit rules apply to all ACLs.

Configuring IP ACLs

Creating an IP ACL

You can create an IPv4 ACL on the switch and add rules to it.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# ip access-list name	Creates the IP ACL and enters IP ACL configuration mode. The <i>name</i> argument can be up to 64 characters.
Step 3	switch(config-acl)# [<i>sequence-number</i>] permit deny } <i>protocol source destination</i>	Creates a rule in the IP ACL. You can create many rules. The <i>sequence-number</i> 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 <i>Command Reference</i> for the specific Cisco Nexus device.
Step 4	(Optional) switch(config-acl)# statistics	Specifies that the switch maintains global statistics for packets that matches the rules in the ACL.
Step 5	(Optional) switch# show ip access-lists name	Displays the IP ACL configuration.
Step 6	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

The following example shows how to create an IPv4 ACL:

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# statistics
```

Changing an IP ACL

You can add and remove rules in an existing IPv4 ACL. You cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes.

If you need to add more rules between existing rules than the current sequence numbering allows, you can use the **resequence** command to reassign sequence numbers.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# ip access-list name	Enters IP ACL configuration mode for the ACL that you specify by name.
Step 3	switch(config)# ip access-list name	Enters IP ACL configuration mode for the ACL that you specify by name.
Step 4	switch(config-acl)# [<i>sequence-number</i>] { permit deny } <i>protocol source destination</i>	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 <i>sequence-number</i> 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 <i>Command Reference</i> for your Cisco Nexus device.
Step 5	(Optional) switch(config-acl)# no [<i>sequence-number</i> { permit deny } <i>protocol source destination</i>]	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 <i>Command Reference</i> for your Cisco Nexus device.
Step 6	(Optional) switch(config-acl)# [no] statistics	Specifies that the switch maintains global statistics for packets that match the rules in the ACL. The no option stops the switch from maintaining global statistics for the ACL.
Step 7	(Optional) switch# show ip access-lists name	Displays the IP ACL configuration.
Step 8	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Related Topics

[Changing Sequence Numbers in an IP ACL](#), on page 76

Removing an IP ACL

You can remove an IP ACL from the switch.

Before you remove an IP ACL from the switch, be sure that you know whether the ACL is applied to an interface. The switch allows you to remove ACLs that are currently applied. Removing an ACL does not affect the configuration of interfaces where you have applied the ACL. Instead, the switch considers the removed ACL to be empty.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# no ip access-list name	Removes the IP ACL that you specified by name from the running configuration.
Step 3	switch(config)# no ip access-list name	Removes the IP ACL that you specified by name from the running configuration.
Step 4	(Optional) switch# show running-config	Displays the ACL configuration. The removed IP ACL should not appear.
Step 5	(Optional) 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.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# resequence ip access-list name starting-sequence-number increment	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 <i>starting-sequence-number</i> argument and the <i>increment</i> argument can be a whole number between 1 and 4294967295.
Step 3	(Optional) switch# show ip access-lists name	Displays the IP ACL configuration.
Step 4	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Applying an IP ACL to mgmt0

You can apply an IPv4 ACL to the management interface (mgmt0).

Before you begin

Ensure that the ACL that you want to apply exists and that it is configured to filter traffic in the manner that you need for this application.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	interface mgmt port Example: <pre>switch(config)# interface mgmt0 switch(config-if)#</pre>	Enters configuration mode for the management interface.
Step 3	ip access-group access-list {in out} Example: <pre>switch(config-if)#ip access-group acl-120 out</pre>	Applies an IPv4 ACL to the Layer 3 interface for traffic flowing in the direction specified. You can apply one router ACL per direction.
Step 4	(Optional) show running-config aclmgr Example: <pre>switch(config-if)# show running-config aclmgr</pre>	Displays the ACL configuration.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

- Creating an IP ACL

Applying an IP ACL as a Port ACL

You can apply an IPv4 ACL to a physical Ethernet interface or a PortChannel. ACLs applied to these interface types are considered port ACLs.



Note Some configuration parameters when applied to an PortChannel are not reflected on the configuration of the member ports.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# interface { ethernet [<i>chassis</i>]/ <i>slot/port</i> port-channel <i>channel-number</i> }	Enters interface configuration mode for the specified interface.
Step 3	switch(config-if)# ip port access-group <i>access-list</i> in	Applies an IPv4 ACL to the interface or PortChannel. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.
Step 4	(Optional) switch# show running-config	Displays the ACL configuration.
Step 5	(Optional) switch# 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 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.



Note Logical operation units (LOUs) are not available for router ACLs applied in the out direction. If an IPv4 ACL is applied as a router ACL in the out direction, access control entries (ACEs) that contain logical operators for TCP/UDP port numbers are expanded internally to multiple ACEs and might require more TCAM entries when compared to the same ACL applied in the in direction.

Before you begin

Ensure that the ACL you want to apply exists and that it is configured to filter traffic in the manner that you need for this application.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 2	Enter one of the following commands: <ul style="list-style-type: none"> • switch(config)# interface ethernet <i>slot/port[. number]</i> • switch(config)# interface port-channel <i>channel-number[. number]</i> • switch(config)# interface tunnel <i>tunnel-number</i> • switch(config)# interface vlan <i>vlan-ID</i> • switch(config)# interface mgmt <i>port</i> 	Enters configuration mode for the interface type that you specified.
Step 3	switch(config-if)# ip access-group <i>access-list {in out}</i>	Applies an IPv4 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.

Verifying IP ACL Configurations

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

Procedure

- switch# **show running-config**

Displays ACL configuration, including IP ACL configuration and interfaces that IP ACLs are applied to.

- switch# **show running-config interface**

Displays the configuration of an interface to which you have applied an ACL.

Example

For detailed information about the fields in the output from these commands, refer to the *Command Reference* for your Cisco Nexus device.

Monitoring and Clearing IP ACL Statistics

Use the **show ip access-lists** command to display statistics about an IP ACL, including the number of packets that have matched each rule. For detailed information about the fields in the output from this command, see the *Command Reference* for your Cisco Nexus device.



Note The mac access-list is applicable to non-IPv4 traffic only.

Procedure

- switch# **show ip access-lists** *name*

Displays IP ACL configuration. If the IP ACL includes the **statistics** command, then the **show ip access-lists** command output includes the number of packets that have matched each rule.

- switch#**show ip access-lists** *name*

Displays IP ACL configuration. If the IP ACL includes the **statistics** command, then the **show ip access-lists** command output includes the number of packets that have matched each rule.

- switch# **clear ip access-list counters** [*access-list-name*]

Clears statistics for all IP ACLs or for a specific IP ACL.

- switch# **clear ip access-list counters** [*access-list-name*]

Clears statistics for all IP ACLs or for a specific IP ACL.

Information About VLAN ACLs

A VLAN ACL (VACL) is one application of an IP ACL. You can configure VACLs to apply to all packets that are bridged within a VLAN. VACLs are used strictly for security packet filtering. VACLs are not defined by direction (ingress or egress).

VACLs and Access Maps

VACLs use access maps to link an IP ACL to an action. The switch takes the configured action on packets that are permitted by the VACL.

VACLs and Actions

In access map configuration mode, you use the **action** command to specify one of the following actions:

- Forward—Sends the traffic to the destination determined by normal operation of the switch.
- Drop—Drops the traffic.

Statistics

The Cisco Nexus device can maintain global statistics for each rule in a VACL. If a VACL is applied to multiple VLANs, the maintained rule statistics are the sum of packet matches (hits) on all the interfaces on which that VACL is applied.



Note The Cisco Nexus device does not support interface-level VACL statistics.

For each VLAN access map that you configure, you can specify whether the switch maintains statistics for that VACL. This allows you to turn VACL statistics on or off as needed to monitor traffic filtered by a VACL or to help troubleshoot VLAN access-map configuration.

Configuring VACLs

Creating or Changing a VACL

You can create or change a VACL. Creating a VACL includes creating an access map that associates an IP ACL with an action to be applied to the matching traffic.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# vlan access-map <i>map-name</i>	Enters access map configuration mode for the access map specified.
Step 3	switch(config-access-map)# match ip address <i>ip-access-list</i>	Specifies an IPv4 ACL for the map.
Step 4	switch(config-access-map)# action { drop forward }	Specifies the action that the switch applies to traffic that matches the ACL.
Step 5	(Optional) switch(config-access-map)# [no] statistics	Specifies that the switch maintains global statistics for packets matching the rules in the VACL. The no option stops the switch from maintaining global statistics for the VACL.
Step 6	(Optional) switch(config-access-map)# show running-config	Displays the ACL configuration.
Step 7	(Optional) switch(config-access-map)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Removing a VACL

You can remove a VACL, which means that you will delete the VLAN access map.

Be sure that you know whether the VACL is applied to a VLAN. The switch allows you to remove VACLs that are current applied. Removing a VACL does not affect the configuration of VLANs where you have applied the VACL. Instead, the switch considers the removed VACL to be empty.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# no vlan access-map <i>map-name</i>	Removes the VLAN access map configuration for the specified access map.
Step 3	(Optional) switch(config)# show running-config	Displays ACL configuration.
Step 4	(Optional) switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Applying a VACL to a VLAN

You can apply a VACL to a VLAN.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# [no] vlan filter <i>map-name</i> vlan-list <i>list</i>	Applies the VACL to the VLANs by the list that you specified. The no option unapplies the VACL. The vlan-list command can specify a list of up to 32 VLANs, but multiple vlan-list commands can be configured to cover more than 32 VLANs.
Step 3	(Optional) switch(config)# show running-config	Displays ACL configuration.
Step 4	(Optional) switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Verifying VACL Configuration

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

Procedure

- switch# **show running-config aclmgr**
Displays ACL configuration, including VACL-related configuration.
- switch# **show vlan filter**
Displays information about VACLs that are applied to a VLAN.

- switch# **show vlan access-map**

Displays information about VLAN access maps.

Displaying and Clearing VACL Statistics

To display or clear VACL statistics, perform one of the following tasks:

Procedure

- switch# **show vlan access-list**

Displays VACL configuration. If the VLAN access-map includes the **statistics** command, then the **show vlan access-list** command output includes the number of packets that have matched each rule.

- switch# **clear vlan access-list counters**

Clears statistics for all VACLs or for a specific VACL.

Configuration Examples for VACL

The following example shows how to configure a VACL to forward traffic permitted by an IP ACL named `acl-ip-01` and how to apply the VACL to VLANs 50 through 82:

```
switch# configure terminal
switch(config)# vlan access-map acl-ip-map
switch(config-access-map)# match ip address acl-ip-01
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# vlan filter acl-ip-map vlan-list 50-82
```

Configuring ACL TCAM Region Sizes

You can change the size of the ACL ternary content addressable memory (TCAM) regions in the hardware.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	hardware profile tcam region {arpacl e-racl} ifacl nat qos} qoslbl racl} vacl } tcam_size	Changes the ACL TCAM region size.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • arpacl—Configures the size of the Address Resolution Protocol (ARP) ACL (ARPAcl) TCAM region. • e-racl—Configures the size of the egress router ACL (ERACL) TCAM region. • e-vacl—Configures the size of the egress VLAN ACL (EVACL) TCAM region. • ifacl—Configures the size of the interface ACL (ifacl) TCAM region. The maximum number of entries is 1500. • nat—Configures the size of the NAT TCAM region. • qos—Configures the size of the quality of service (QoS) TCAM region. • qoslbl—Configures the size of the QoS Label (qoslbl) TCAM region. • racl—Configures the size of the router ACL (RAcl) TCAM region. • vacl—Configures the size of the VLAN ACL (VAcl) TCAM region. • tcam_size—TCAM size. The range is from 0 to 2,14,74, 83, 647 entries. <p>Note vacl and e-vacl TCAM regions should be set to the same size.</p>
Step 3	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.
Step 4	<pre>switch(config)# show hardware profile tcam region</pre> Example: <pre>switch(config)# show hardware profile tcam region</pre>	Displays the TCAM sizes that will be applicable on the next reload of the switch.
Step 5	<pre>switch(config)# reload</pre> Example: <pre>switch(config)# reload</pre>	Copies the running configuration to the startup configuration. <p>Note The new size values are effective only upon the next reload after saving the copy running-config to startup-config.</p>

Example

The following example shows how to change the size of the RAACL TCAM region:

```
switch(config)# hardware profile tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'
```

```
switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

The following example shows how to configure the TCAM VLAN ACLs on a switch:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# hardware profile tcam region vacl 512
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'
```

```
switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

This example shows how to display the TCAM region sizes to verify your changes:

```
switch(config)# show hardware profile tcam region
  sup size = 16
  vacl size = 640
  ifacl size = 496
  qos size = 256
  rbacl size = 0
  span size = 0
  racl size = 1536
  e-racl size = 256
  e-vacl size = 640
  qoslbl size = 0
  arpacl size = 0
```

This example shows how to determine TCAM utilization for particular region. There are 5 RAACL entries in this example:

```
switch(config)# show platform afm info tcam 0 racl
  racl TCAM configuration for ASIC id 0:
[   sup tcam]: range 0 - 47
[   vacl tcam]: range 512 - 1087
[   ifacl tcam]: range 112 - 511
[   qos tcam]: range 3712 - 3903
[   rbacl tcam]: range 0 - 0
[   span tcam]: range 0 - 0
[   racl tcam]: range 1984 - 3455 *
[   e-racl tcam]: range 3456 - 3711
[   e-vacl tcam]: range 1088 - 1727
[   qoslbl tcam]: range 0 - 0
[   ipsg tcam]: range 0 - 0
[   arpacl tcam]: range 0 - 0
[   ipv6-racl tcam]: range 0 - 0
[   ipv6-e-racl tcam]: range 0 - 0
[   ipv6-sup tcam]: range 0 - 0
[   ipv6-qos tcam]: range 0 - 0
[   nat tcam]: range 1728 - 1983
```

```

[      e-qos tcam]: range  3904 - 3967
[      pbr tcam]: range    0 -    0
[  ipv6-pbr tcam]: range    0 -    0
[      copp tcam]: range   48 -  111

TCAM [racl tcam]: [v:1, size:1472, start:1984 end:3455]
In use tcam entries: 5
                 3451-3455
Link Local Entries:

```

Reverting to the Default TCAM Region Sizes

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	switch(config)# no hardware profile tcam region {arpacl e-racl} ifacl nat qos} qoslbl racl} vacl } tcam_size	Reverts the configuration to the default ACL TCAM size.
Step 3	(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.
Step 4	switch(config)# reload	Reloads the switch.

Example

The following example shows how to revert to the default RAcl TCAM region sizes:

```

switch(config)# no hardware profile tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y

```

Configuring ACLs on Virtual Terminal Lines

To restrict incoming and outgoing connections for IPv4 between a Virtual Terminal (VTY) line and the addresses in an access list, use the **access-class** command in line configuration mode. To remove access restrictions, use the **no** form of this command.

Follow these guidelines when configuring ACLs on VTY lines:

- Set identical restrictions on all VTY lines because a user can connect to any of them.
- Statistics per entry is not supported for ACLs on VTY lines.

Before you begin

Be sure that the ACL that you want to apply exists and is configured to filter traffic for this application.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# line vty Example: switch(config)# line vty switch(config-line)#	Enters line configuration mode.
Step 3	switch(config-line)# access-class access-list-number {in out} Example: switch(config-line)# access-class ozi2 in switch(config-line)# access-class ozi3 out switch(config)#	Specifies inbound or outbound access restrictions.
Step 4	(Optional) switch(config-line)# no access-class access-list-number {in out} Example: switch(config-line)# no access-class ozi2 in switch(config-line)# no access-class ozi3 out switch(config)#	Removes inbound or outbound access restrictions.
Step 5	switch(config-line)# exit Example: switch(config-line)# exit switch#	Exits line configuration mode.
Step 6	(Optional) switch# show running-config aclmgr Example: switch# show running-config aclmgr	Displays the running configuration of the ACLs on the switch.
Step 7	(Optional) switch# copy running-config startup-config Example:	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	switch# copy running-config startup-config	

Example

The following example shows how to apply the access-class ozi2 command to the in-direction of the vty line.

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# line vty
switch(config-line)# access-class ozi2 in
switch(config-line)# exit
switch#
```

Verifying ACLs on VTY Lines

To display the ACL configurations on VTY lines, perform one of the following tasks:

Command	Purpose
show running-config aclmgr	Displays the running configuration of the ACLs configured on the switch.
show users	Displays the users that are connected.
show access-lists <i>access-list-name</i>	Display the statistics per entry.

Configuration Examples for ACLs on VTY Lines

The following example shows the connected users on the console line (ttyS0) and the VTY lines (pts/0 and pts/1).

```
switch# show users
NAME      LINE      TIME          IDLE          PID COMMENT
admin     ttyS0     Aug 27 20:45  .             14425 *
admin     pts/0     Aug 27 20:06 00:46        14176 (172.18.217.82) session=ssh
admin     pts/1     Aug 27 20:52  .             14584 (10.55.144.118)
```

The following example shows how to allow vty connections to all IPv4 hosts except 172.18.217.82 and how to deny vty connections to any IPv4 host except 10.55.144.118, 172.18.217.79, 172.18.217.82, 172.18.217.92:

```
switch# show running-config aclmgr
!Time: Fri Aug 27 22:01:09 2010
version 5.0(2)N1(1)
ip access-list ozi
 10 deny ip 172.18.217.82/32 any
 20 permit ip any any
ip access-list ozi2
 10 permit ip 10.55.144.118/32 any
 20 permit ip 172.18.217.79/32 any
 30 permit ip 172.18.217.82/32 any
 40 permit ip 172.18.217.92/32 any
```

```
line vty
  access-class ozi in
  access-class ozi2 out
```

The following example shows how to configure the IP access list by enabling per-entry statistics for the ACL:

```
switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
switch(config)# ip access-list ozi2
switch(config-acl)# statistics per-entry
switch(config-acl)# deny tcp 172.18.217.83/32 any
switch(config-acl)# exit

switch(config)# ip access-list ozi
switch(config-acl)# statistics per-entry
switch(config-acl)# permit ip 172.18.217.20/24 any
switch(config-acl)# exit
switch#
```

The following example shows how to apply the ACLs on VTY in and out directions:

```
switch(config)# line vty
switch(config-line)# ip access-class ozi in
switch(config-line)# access-class ozi2 out
switch(config-line)# exit
switch#
```

The following example shows how to remove the access restrictions on the VTY line:

```
switch# configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
switch(config)# line vty
switch(config-line)# no access-class ozi2 in
switch(config-line)# no ip access-class ozi2 in
switch(config-line)# exit
switch#
```




CHAPTER 8

Configuring DHCP Snooping

This chapter includes the following sections:

- [Information About DHCP Snooping, on page 91](#)
- [Information About the DHCP Relay Agent, on page 93](#)
- [Licensing Requirements for DHCP Snooping, on page 94](#)
- [Prerequisites for DHCP Snooping, on page 94](#)
- [Guidelines and Limitations for DHCP Snooping, on page 95](#)
- [Default Settings for DHCP Snooping, on page 95](#)
- [Configuring DHCP Snooping, on page 95](#)
- [Verifying the DHCP Snooping Configuration, on page 108](#)
- [Displaying DHCP Bindings, on page 108](#)
- [Clearing the DHCP Snooping Binding Database, on page 109](#)
- [Clearing DHCP Relay Statistics, on page 110](#)
- [Monitoring DHCP, on page 110](#)
- [Configuration Examples for DHCP Snooping, on page 110](#)

Information About DHCP Snooping

DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers. DHCP snooping performs the following activities:

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
- Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
- Uses the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

Feature Enabled and Globally Enabled

When you are configuring DHCP snooping, it is important that you understand the difference between enabling the DHCP snooping feature and globally enabling DHCP snooping.

Feature Enablement

The DHCP snooping feature is disabled by default. When the DHCP snooping feature is disabled, you cannot configure it or any of the features that depend on DHCP snooping. The commands to configure DHCP snooping and its dependent features are unavailable when DHCP snooping is disabled.

When you enable the DHCP snooping feature, the switch begins building and maintaining the DHCP snooping binding database. Features dependent on the DHCP snooping binding database can now make use of it and can therefore also be configured.

Enabling the DHCP snooping feature does not globally enable it. You must separately enable DHCP snooping globally.

Disabling the DHCP snooping feature removes all DHCP snooping configuration from the switch. If you want to disable DHCP snooping and preserve the configuration, globally disable DHCP snooping but do not disable the DHCP snooping feature.

Global Enablement

After DHCP snooping is enabled, DHCP snooping is globally disabled by default. Global enablement is a second level of enablement that allows you to have separate control of whether the switch is actively performing DHCP snooping that is independent from enabling the DHCP snooping binding database.

When you globally enable DHCP snooping, on each untrusted interface of VLANs that have DHCP snooping enabled, the switch begins validating DHCP messages that are received and used the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

When you globally disable DHCP snooping, the switch stops validating DHCP messages and validating subsequent requests from untrusted hosts. It also removes the DHCP snooping binding database. Globally disabling DHCP snooping does not remove any DHCP snooping configuration or the configuration of other features that are dependent upon the DHCP snooping feature.

Trusted and Untrusted Sources

You can configure whether DHCP snooping trusts traffic sources. An untrusted source might initiate traffic attacks or other hostile actions. To prevent such attacks, DHCP snooping filters messages from untrusted sources.

In an enterprise network, a trusted source is a switch that is under your administrative control. These switches include the switches, routers, and servers in the network. Any switch beyond the firewall or outside the network is an untrusted source. Generally, host ports are treated as untrusted sources.

In a service provider environment, any switch that is not in the service provider network is an untrusted source (such as a customer switch). Host ports are untrusted sources.

In a Cisco Nexus device, you indicate that a source is trusted by configuring the trust state of its connecting interface.

The default trust state of all interfaces is untrusted. You must configure DHCP server interfaces as trusted. You can also configure other interfaces as trusted if they connect to switches (such as switches or routers) inside your network. You usually do not configure host port interfaces as trusted.



Note For DHCP snooping to function properly, you must connect all DHCP servers to the switch through trusted interfaces.

DHCP Snooping Binding Database

Using information extracted from intercepted DHCP messages, DHCP snooping dynamically builds and maintains a database. The database contains an entry for each untrusted host with a leased IP address if the host is associated with a VLAN that has DHCP snooping enabled. The database does not contain entries for hosts that are connected through trusted interfaces.



Note The DHCP snooping binding database is also referred to as the DHCP snooping binding table.

DHCP snooping updates the database when the switch receives specific DHCP messages. For example, the feature adds an entry to the database when the switch receives a DHCPACK message from the server. The feature removes the entry in the database when the IP address lease expires or the switch receives a DHCPRELEASE message from the host.

Each entry in the DHCP snooping binding database includes the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host.

You can remove entries from the binding database by using the **clear ip dhcp snooping binding** command.

Information About the DHCP Relay Agent

DHCP Relay Agent

You can configure the device to run a DHCP relay agent, which forwards DHCP packets between clients and servers. This feature is useful when clients and servers are not on the same physical subnet. Relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The relay agent sets the gateway address (giaddr field of the DHCP packet) and, if configured, adds the relay agent information option (Option 82) in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing Option 82.

After you enable Option 82, the device uses the binary ifindex format by default. If needed, you can change the Option 82 setting to use an encoded string format instead.



Note When the device relays a DHCP request that already includes Option 82 information, the device forwards the request with the original Option 82 information without altering it.

VRF Support for the DHCP Relay Agent

You can configure the DHCP relay agent to forward DHCP broadcast messages from clients in a virtual routing and forwarding (VRF) instance to DHCP servers in a different VRF. By using a single DHCP server to provide DHCP support to clients in multiple VRFs, you can conserve IP addresses by using a single IP address pool rather than one for each VRF.

Enabling VRF support for the DHCP relay agent requires that you enable Option 82 for the DHCP relay agent.

If a DHCP request arrives on an interface that you have configured with a DHCP relay address and VRF information, and the address of the DHCP server belongs to a network on an interface that is a member of a different VRF, the device inserts Option 82 information in the request and forwards it to the DHCP server in the server VRF. The Option 82 information includes the following:

VPN identifier

Name of the VRF that the interface that receives the DHCP request is a member of.

Link selection

Subnet address of the interface that receives the DHCP request.

Server identifier override

IP address of the interface that receives the DHCP request.



Note The DHCP server must support the VPN identifier, link selection, and server identifier override options.

When the device receives the DHCP response message, it strips off the Option 82 information and forwards the response to the DHCP client in the client VRF.

DHCP Relay Binding Database

A relay binding is an entity that associates a DHCP or BOOTP client with a relay agent address and its subnet. Each relay binding stores the client MAC address, active relay agent address, active relay agent address mask, logical and physical interfaces to which the client is connected, giaddr retry count, and total retry count. The giaddr retry count is the number of request packets transmitted with that relay agent address, and the total retry count is the total number of request packets transmitted by the relay agent. One relay binding entry is maintained for each DHCP or BOOTP client.



Note When DHCP smart relay is enabled globally or at the interface level on any switch, the relay bindings on all switches should be synchronized with the vPC peer.

Licensing Requirements for DHCP Snooping

This feature does not require a license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Prerequisites for DHCP Snooping

You should be familiar with DHCP before you configure DHCP snooping or the DHCP relay agent .

Guidelines and Limitations for DHCP Snooping

Consider the following guidelines and limitations when configuring DHCP snooping:

- The DHCP snooping database can store 2000 bindings.
- DHCP snooping is not active until you enable the feature, enable DHCP snooping globally, and enable DHCP snooping on at least one VLAN.
- Before globally enabling DHCP snooping on the switch, make sure that the switches that act as the DHCP server and the DHCP relay agent are configured and enabled.
- If a VLAN ACL (VACL) is configured on a VLAN that you are configuring with DHCP snooping, ensure that the VACL permits DHCP traffic between DHCP servers and DHCP hosts.
- DHCP snooping and DHCP relay feature are not supported on the same VLAN.

Default Settings for DHCP Snooping

This table lists the default settings for DHCP snooping parameters.

Table 13: Default DHCP Snooping Parameters

Parameters	Default
DHCP snooping feature	Disabled
DHCP snooping globally enabled	No
DHCP snooping VLAN	None
DHCP snooping Option 82 support	Disabled
DHCP snooping trust	Untrusted
VRF support for the DHCP relay agent	Disabled
DHCP relay agent	Disabled

Configuring DHCP Snooping

Minimum DHCP Snooping Configuration

1. Enable the DHCP snooping feature.
- 2.

Procedure

	Command or Action	Purpose
Step 1	Enable the DHCP snooping feature.	When the DHCP snooping feature is disabled, you cannot configure DHCP snooping. For details, see Enabling or Disabling the DHCP Snooping Feature , on page 96.
Step 2	Enable DHCP snooping globally.	For details, see Enabling or Disabling DHCP Snooping Globally , on page 97.
Step 3	Enable DHCP snooping on at least one VLAN.	By default, DHCP snooping is disabled on all VLANs. For details, see Enabling or Disabling DHCP Snooping on a VLAN , on page 97.
Step 4	Ensure that the DHCP server is connected to the switch using a trusted interface.	For details, see Configuring an Interface as Trusted or Untrusted , on page 101.

Enabling or Disabling the DHCP Snooping Feature

You can enable or disable the DHCP snooping feature on the switch. By default, DHCP snooping is disabled.

Before you begin

If you disable the DHCP snooping feature, all DHCP snooping configuration is lost. If you want to turn off DHCP snooping and preserve the DHCP snooping configuration, disable DHCP globally.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no] feature dhcp Example: <pre>switch(config)# feature dhcp</pre>	Enables the DHCP snooping feature. The no option disables the DHCP snooping feature and erases all DHCP snooping configuration.
Step 3	(Optional) show running-config dhcp Example: <pre>switch(config)# show running-config dhcp</pre>	Shows the DHCP snooping configuration.
Step 4	(Optional) copy running-config startup-config Example:	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	<code>switch(config)# copy running-config startup-config</code>	

Enabling or Disabling DHCP Snooping Globally

You can enable or disable the DHCP snooping globally on the switch. Globally disabling DHCP snooping stops the switch from performing any DHCP snooping or relaying DHCP messages but preserves DHCP snooping configuration.

Before you begin

Ensure that you have enabled the DHCP snooping feature. By default, DHCP snooping is globally disabled.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
Step 2	[no] ip dhcp snooping Example: <code>switch(config)# ip dhcp snooping</code>	Enables DHCP snooping globally. The no option disables DHCP snooping.
Step 3	(Optional) show running-config dhcp Example: <code>switch(config)# show running-config dhcp</code>	Shows the DHCP snooping configuration.
Step 4	(Optional) copy running-config startup-config Example: <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Enabling or Disabling DHCP Snooping on a VLAN

You can enable or disable DHCP snooping on one or more VLANs.

Before you begin

By default, DHCP snooping is disabled on all VLANs.

Ensure that DHCP snooping is enabled.



Note If a VACL is configured on a VLAN that you are configuring with DHCP snooping, ensure that the VACL permits DHCP traffic between DHCP servers and DHCP hosts.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no] ip dhcp snooping vlan <i>vlan-list</i> Example: <pre>switch(config)# ip dhcp snooping vlan 100,200,250-252</pre>	Enables DHCP snooping on the VLANs specified by <i>vlan-list</i> . The no option disables DHCP snooping on the VLANs specified.
Step 3	(Optional) show running-config dhcp Example: <pre>switch(config)# show running-config dhcp</pre>	Shows the DHCP snooping configuration.
Step 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

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.

Before you begin

Ensure that the DHCP feature is enabled.

Procedure

	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) [no] ip dhcp snooping sub-option circuit-id format-type string format Example: switch(config)# ip dhcp snooping sub-option circuit-id format-type string format	Configures Option 82 to use encoded string format of either ingress ifindex name or host name or a combination of both hostname and ifindex name. [“%h” for hostname, “%p” for ifindex and combination of %h and %p for both hostname and ifindex name.
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 Option 82 User Defined Data Insertion and Removal

You can enable or disable the insertion and removal of Option 82 user-defined information for DHCP packets forwarded to server. The configuration is applicable per port and overrides option82 global configuration that uses encoded string format of ingress ifindex name. When DHCP Relay is configured on SVI, the user defined string from the ingress physical *ifindex* is appended to the DHCP Packet being relayed.

By default, the device does not include option 82 information in DHCP packets.



Note The user-defined option82 configuration applies to both DHCP Relay and DHCP Snooping.

Before you begin

Ensure that the DHCP feature is enabled.

Procedure

	Command or Action	Purpose
Step 1	<code>config t</code>	Enters global configuration mode.
Step 2	<code>[no] ip dhcp snooping information option</code>	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	<code>interface ethernet slot/port</code>	Enters interface configuration mode, where slot/port is the Layer 2 Ethernet ingress interface where you want to configure the option 82 string.
Step 4	<code>ip dhcp option82 suboption circuit-id user-defined-circuit-id</code> Example: <code>switch(config-if)# ip dhcp option82 suboption circuit-id po5-option82-string</code>	Enters user defined option82 string on port channel5. The string po5-option82-string is appended to the DHCP Packet being ingress on port channel 5. The same is configured on Ethernet interface.
Step 5	(Optional) <code>show ip dhcp option82 suboption info interface po5</code>	Displays the DHCP option 82 information and statistics.
Step 6	(Optional) <code>copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Enabling or Disabling Strict DHCP Packet Validation

You can enable or disable the strict validation of DHCP packets by the DHCP snooping feature. By default, strict validation of DHCP packets is disabled.

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code> Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
Step 2	<code>[no] ip dhcp packet strict-validation</code> Example: <code>switch(config)# ip dhcp packet strict-validation</code>	Enables the strict validation of DHCP packets by the DHCP snooping feature. The no option disables strict DHCP packet validation.
Step 3	(Optional) <code>show running-config dhcp</code> Example: <code>switch(config)# show running-config dhcp</code>	Shows the DHCP snooping configuration.

	Command or Action	Purpose
Step 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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. You can configure DHCP trust on the following types of interfaces:

- Layer 2 Ethernet interfaces
- Layer 2 port-channel interfaces

Before you begin

By default, all interfaces are untrusted.

Ensure that DHCP snooping is enabled.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	Enter one of the following commands: <ul style="list-style-type: none"> • interface ethernet <i>port/slot</i> • interface port-channel <i>channel-number</i> Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	<ul style="list-style-type: none"> • Enters interface configuration mode, where <i>port / slot</i> is the Layer 2 Ethernet interface that you want to configure as trusted or untrusted for DHCP snooping. • Enters interface configuration mode, where <i>port / slot</i> 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: <pre>switch(config-if)# ip dhcp snooping trust</pre>	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: <pre>switch(config-if)# show running-config dhcp</pre>	Shows the DHCP snooping configuration.

	Command or Action	Purpose
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.

Enabling or Disabling the DHCP Relay Agent

You can enable or disable the DHCP relay agent. By default, the DHCP relay agent is enabled.

Before you begin

Ensure that the DHCP feature is enabled.

Procedure

	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.
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 Option 82 for the DHCP Relay Agent

You can enable or disable the device to insert and remove Option 82 information on DHCP packets forwarded by the relay agent.

By default, the DHCP relay agent does not include Option 82 information in DHCP packets.

Procedure

	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.

Procedure

	Command or Action	Purpose
Step 1	config t Example:	Enters global configuration mode.

	Command or Action	Purpose
	switch# config t switch(config)#	
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: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Enabling or Disabling Subnet Broadcast Support for the DHCP Relay Agent on a Layer 3 Interface

You can configure the device to support the relaying of DHCP packets from clients to a subnet broadcast IP address. When this feature is enabled, the VLAN ACLs (VACLs) accept IP broadcast packets and all subnet broadcast (primary subnet broadcast as well as secondary subnet broadcast) packets.

Before you begin

Ensure that the DHCP feature is enabled.

Ensure that the DHCP relay agent is enabled.

Procedure

	Command or Action	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters global configuration mode.
Step 2	interface <i>interface slot/port</i> Example: switch(config)# interface ethernet 2/2 switch(config-if)#	Enters interface configuration mode, where <i>slot/port</i> 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.
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.

Procedure

	Command or Action	Purpose
Step 1	config t Example: <pre>switch# config t switch(config)#</pre>	Enters global configuration mode.
Step 2	Do one of the following options: <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i>[. <i>number</i>] • interface vlan <i>vlan-id</i> • interface port-channel <i>channel-id</i>[. <i>subchannel-id</i>] Example: <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	<ul style="list-style-type: none"> • Enters interface configuration mode, where <i>slot/port</i> 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 <i>number</i> argument to specify the subinterface number. • Enters interface configuration mode, where <i>vlan-id</i> is the ID of the VLAN that you want to configure with a DHCP server IP address. • Enters interface configuration mode, where <i>channel-id</i> 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 <i>subchannel-id</i> argument to specify the subchannel ID.
Step 3	ip dhcp relay address <i>IP-address</i> [use-vrf <i>vrf-name</i>] Example: <pre>switch(config-if)# ip dhcp relay address 10.132.7.120 use-vrf red</pre>	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.

	Command or Action	Purpose
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: switch(config-if)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Creating a DHCP Static Binding

You can create a static DHCP source binding to a Layer 2 interface.

Before you begin

Ensure that you have enabled the DHCP snooping feature.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	ip source binding <i>IP-address MAC-address</i> vlan <i>vlan-id</i> { interface ethernet <i>slot/port</i> port-channel <i>channel-no</i> } Example: switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet 2/3	Binds the static source address to the Layer 2 Ethernet interface.
Step 3	(Optional) show ip dhcp snooping binding Example: switch(config)# ip dhcp snooping binding	Shows the DHCP snooping static and dynamic bindings.
Step 4	(Optional) show ip dhcp snooping binding dynamic	Shows the DHCP snooping dynamic bindings.

	Command or Action	Purpose
	Example: <pre>switch(config)# ip dhcp snooping binding dynamic</pre>	
Step 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Example

The following example shows how to create a static IP source entry associated with VLAN 100 on Ethernet interface 2/3:

```
switch# configure terminal
switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet 2/3
switch(config)#
```

Verifying the DHCP Snooping Configuration

To display DHCP snooping configuration information, perform one of the following tasks. For detailed information about the fields in the output from these commands, see the System Management Configuration Guide for your Cisco Nexus device.

Command	Purpose
show running-config dhcp	Displays the DHCP snooping configuration.
show ip dhcp relay	Displays the DHCP relay configuration.
show ip dhcp snooping	Displays general information about DHCP snooping.

Displaying DHCP Bindings

Use the **show ip dhcp snooping binding** command to display the DHCP static and dynamic binding table. Use the **show ip dhcp snooping binding dynamic** to display the DHCP dynamic binding table.

For detailed information about the fields in the output from this command, see the *System Management Configuration Guide* for your Cisco Nexus device.

This example shows how to create a static DHCP binding and then verify the binding using the **show ip dhcp snooping binding** command.


```

switch# configuration terminal
switch(config)# ip source binding 10.20.30.40 0000.1111.2222 vlan 400 interface port-channel
500

switch(config)# show ip dhcp snooping binding
MacAddress      IPAddress      LeaseSec      Type          VLAN    Interface
-----
00:00:11:11:22:22  10.20.30.40    infinite      static        400     port-channel500

```

Clearing the DHCP Snooping Binding Database

You can remove entries from the DHCP snooping binding database, including a single entry, all entries associated with an interface, or all entries in the database.

Before you begin

Ensure that DHCP snooping is enabled.

Procedure

	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 <i>slot/port[.subinterface-number]</i> 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 <i>channel-number[.subchannel-number]</i> 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 <i>vlan-id</i> mac <i>mac-address</i> ip <i>ip-address</i> interface {ethernet <i>slot/port[.subinterface-number]</i> port-channel <i>channel-number[.subchannel-number]</i> } 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.

	Command or Action	Purpose
Step 5	(Optional) show ip dhcp snooping binding Example: switch# show ip dhcp snooping binding	Displays the DHCP snooping binding database.

Clearing DHCP Relay Statistics

Use the **clear ip dhcp relay statistics** command to clear the global DHCP relay statistics.

Use the **clear ip dhcp relay statistics interface *interface*** command to clear the DHCP relay statistics for a particular interface.

Use the **clear ip dhcp relay statistics interface *interface* serverip *ip-address* [use-vrf *vrf-name*]** command to clear the DHCP relay statistics at the server level for a particular interface.

Monitoring DHCP

Use the **show ip dhcp snooping statistics** command to monitor DHCP snooping.

Use the **show ip dhcp relay statistics [interface *interface* [serverip *ip-address* [use-vrf *vrf-name*]]]** command to monitor DHCP relay statistics at the global, server, or interface level.

Use the (Optional) **show ip dhcp snooping statistics vlan [vlan-id] interface [ethernet|port-channel][*id*]** command to know the exact statistics about snooping statistics per interface under a vlan.

Configuration Examples for DHCP Snooping

The following example shows how to enable DHCP snooping on two VLANs, with Option 82 support enabled and Ethernet interface 2/5 trusted because the DHCP server is connected to that interface:

```
feature dhcp
ip dhcp snooping
ip dhcp snooping info option

interface Ethernet 2/5
 ip dhcp snooping trust
ip dhcp snooping vlan 1
ip dhcp snooping vlan 50
```



CHAPTER 9

Configuring MAC ACLs

This chapter describes how to configure MAC access lists (ACLs) on Cisco NX-OS devices.

This chapter contains the following sections:

- [Information About MAC ACLs, on page 111](#)
- [Default Settings for MAC ACLs, on page 112](#)
- [Configuring MAC ACLs, on page 112](#)
- [Verifying the MAC ACL Configuration, on page 118](#)
- [Clearing MAC ACL Statistics, on page 119](#)

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.

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	<ul style="list-style-type: none">• A MAC ACL that is on the interface applies to all traffic entering the interface, including IP traffic.• You can apply an IP port ACL on the interface, but it will not filter traffic.
Disabled	<ul style="list-style-type: none">• 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 and it will filter traffic.

Default Settings for MAC ACLs

This table lists the default settings for MAC ACL parameters.

Table 14: 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.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# mac access-list name	Creates the MAC ACL and enters ACL configuration mode.
Step 3	switch(config-mac-acl)# {permit deny} <i>source destination protocol</i>	Creates a rule in the MAC ACL. The permit and deny commands support many ways of identifying traffic.
Step 4	(Optional) 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) switch(config-mac-acl)# show mac access-lists name	Displays the MAC ACL configuration.
Step 6	(Optional) switch(config-mac-acl)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

This example shows how to create a MAC ACL:

```
switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any
```

```

switch(config-mac-acl)# statistics per-entry
switch(config-mac-acl)# show mac access-lists acl-mac-01

MAC ACL acl-mac-01
    statistics per-entry
    10 permit 00c0.4f00.0000 0000.00ff.ffff any

switch(config-mac-acl)# copy running-config startup-config

```

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.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# mac access-list name	Enters ACL configuration mode for the ACL that you specify by name.
Step 3	(Optional) switch(config-mac-acl)# [<i>sequence-number</i>] {permit deny} <i>source destination protocol</i>	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.
Step 4	(Optional) switch(config-mac-acl)# no { <i>sequence-number</i> {permit deny} } <i>source destination protocol</i> }	Removes the rule that you specify from the MAC ACL. The permit and deny commands support many ways of identifying traffic.
Step 5	(Optional) switch(config-mac-acl)# [no] 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 6	(Optional) switch(config-mac-acl)# show mac access-lists name	Displays the MAC ACL configuration.
Step 7	(Optional) switch(config-mac-acl)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

This example shows how to change a MAC ACL:

```

switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# 100 permit 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# 80 permit 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# no 80
switch(config-mac-acl)# statistics per-entry
switch(config-mac-acl)# show mac access-lists acl-mac-01

MAC ACL acl-mac-01
    statistics per-entry
    10 permit 00c0.4f00.0000 0000.00ff.ffff any
    100 permit 00c0.4f00.0000 0000.00ff.ffff any

switch(config-mac-acl)# copy running-config startup-config

```

Changing Sequence Numbers in a MAC ACL

You can change all the sequence numbers assigned to rules in a MAC ACL. Resequencing is useful when you need to insert rules into an ACL and there are not enough available sequence numbers.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# resequence mac access-list name starting-sequence-number increment	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) switch(config)# show mac access-lists name	Displays the MAC ACL configuration.
Step 4	(Optional) switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

This example shows how to change the sequence of a MAC ACL:

```

switch# configure terminal
switch(config)# resequence mac access-list acl-mac-01 100 15
switch(config)# show mac access-lists acl-mac-01

```

```

MAC ACL acl-mac-01
  statistics per-entry
  100 permit 00c0.4f00.0000 0000.00ff.ffff any
  115 permit 00c0.4f00.0000 0000.00ff.ffff any

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

```

Removing a MAC ACL

You can remove a MAC ACL from the device.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# no mac access-list name	Removes the MAC ACL that you specify by name from the running configuration.
Step 3	(Optional) switch(config)# show mac access-lists name summary	Displays the MAC ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.
Step 4	(Optional) switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

This example shows how to remove a MAC ACL:

```

switch# configure terminal
switch(config)# show mac access-lists

MAC ACL acl-mac-01
  statistics per-entry
  100 permit 00c0.4f00.0000 0000.00ff.ffff any
  115 permit 00c0.4f00.0000 0000.00ff.ffff any
MAC ACL acl-mac-02
  statistics per-entry
  10 permit 00a0.3f00.0000 0000.00dd.ffff any
MAC ACL acl-mac-03
  statistics per-entry
  10 permit 00b0.5f00.0000 0000.00aa.fbbf any

switch(config)# no mac access-list acl-mac-02
switch(config)# show mac access-lists acl-mac-02 summary
switch(config)# show mac access-lists

MAC ACL acl-mac-01
  statistics per-entry
  100 permit 00c0.4f00.0000 0000.00ff.ffff any
  115 permit 00c0.4f00.0000 0000.00ff.ffff any
MAC ACL acl-mac-03
  statistics per-entry
  10 permit 00b0.5f00.0000 0000.00aa.fbbf any

```

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

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.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	Enter one of the following commands: <ul style="list-style-type: none"> • switch(config)# interface ethernet slot/port • switch(config)# interface port-channel channel-number 	<ul style="list-style-type: none"> • 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	switch(config-if)# mac port access-group access-list	Applies a MAC ACL to the interface.
Step 4	(Optional) switch(config-if)# show running-config aclmgr	Displays ACL configuration.
Step 5	(Optional) switch(config-if)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

This example shows how to apply a MAC ACL as a port ACL to an Ethernet interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# mac port access-group acl-mac-01
switch(config-if)# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Sat Jul 19 23:36:04 2014

version 6.0(2)A4(1)
mac access-list acl-mac-01
  statistics per-entry
  100 permit 00C0.4F00.0000 0000.00FF.FFFF any
```



```

    115 permit 00C0.4F00.0000 0000.00FF.FFFF any
mac access-list acl-mac-03
  statistics per-entry
    10 permit 00B0.5F00.0000 0000.00AA.FBBF any
ip access-list copp-system-acl-bfd
  10 permit udp any any eq 3784
ip access-list copp-system-acl-eigrp
  10 permit eigrp any any
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any
...

interface Ethernet1/3
  mac port access-group acl-mac-01

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

```

This example shows how to apply a MAC ACL as a port ACL to a port-channel interface:

```

switch# configure terminal
switch(config)# interface port-channel 5
switch(config-if)# mac port access-group acl-mac-01
switch(config-if)# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Sat Jul 19 23:37:04 2014

version 6.0(2)A4(1)
mac access-list acl-mac-01
  statistics per-entry
    100 permit 00C0.4F00.0000 0000.00FF.FFFF any
    115 permit 00C0.4F00.0000 0000.00FF.FFFF any
mac access-list acl-mac-03
  statistics per-entry
    10 permit 00B0.5F00.0000 0000.00AA.FBBF any
ip access-list copp-system-acl-bfd
  10 permit udp any any eq 3784
ip access-list copp-system-acl-eigrp
  10 permit eigrp any any
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any
...

interface port-channel5
  mac port access-group acl-mac-01

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

```

Enabling or Disabling MAC Packet Classification

You can enable or disable MAC packet classification on a per VLAN basis.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# feature interface-vlan	Enables the interface-vlan feature.
Step 3	switch(config)# interface vlan <i>interface-vlan-number</i>	Creates a VLAN interface. The number range is from 1 to 4094.
Step 4	switch(config-if)# [no] mac packet-classify	Enables MAC packet classification on the interface. The no option disables MAC packet classification on the interface.
Step 5	(Optional) switch(config-if)# show running-config interface vlan <i>interface-vlan-number</i>	Displays the running configuration of the VLAN interface.
Step 6	(Optional) switch(config-if)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

This example shows how to enable MAC packet classification on a per VLAN basis:

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# interface vlan 50
switch(config-if)# mac packet-classify
switch(config-if)# show running-config interface vlan 50

!Command: show running-config interface Vlan50
!Time: Wed Aug 6 20:39:03 2014

version 6.0(2)A4(1)

interface Vlan50
  mac packet-classify

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

Verifying the MAC ACL Configuration

To display MAC ACL configuration information, perform one of the following tasks.

Command	Purpose
show mac access-lists	Displays the MAC ACL configuration.

Command	Purpose
<code>show running-config aclmgr [all]</code>	<p>Displays the ACL configuration, including MAC ACLs and the interfaces to which MAC ACLs are applied.</p> <p>Note The all option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.</p>
<code>show startup-config aclmgr [all]</code>	<p>Displays the ACL startup configuration.</p> <p>Note The all option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.</p>

Clearing MAC ACL Statistics

You can clear MAC ACL statistics by using the `clear mac access-list counters` command

Command	Purpose
<code>clear mac access-list counters</code>	Clears statistics for all MAC ACLs or for a specific MAC ACL.



CHAPTER 10

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:

- [Information About Unicast RPF, on page 121](#)
- [Licensing Requirements for Unicast RPF, on page 122](#)
- [Guidelines and Limitations for Unicast RPF, on page 122](#)
- [Default Settings for Unicast RPF, on page 123](#)
- [Configuring Unicast RPF, on page 123](#)
- [Configuration Examples for Unicast RPF, on page 124](#)
- [Verifying the Unicast RPF Configuration, on page 125](#)

Information About Unicast RPF

The Unicast RPF feature reduces problems that are caused by the introduction of malformed or forged (spoofed) IPv4 source addresses into a network by discarding IPv4 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 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 switch 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 switch at the upstream end of a connection.

Unicast RPF verifies that any packet received at a switch 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

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.

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.

Licensing Requirements for Unicast RPF

Product	License Requirement
Cisco NX-OS	Unicast RPF 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 <i>Cisco NX-OS Licensing Guide</i> .

Guidelines and Limitations for Unicast RPF

Unicast RPF has the following configuration guidelines and limitations:

- In Warp mode that is unique to Cisco Nexus 3548 Series switches, when URPF is enabled, the number of multicast entries is halved from 8k to 4k. Similarly, the number of host entries is also halved from 8k to 4k. In Normal mode, the number of LPM entries supported is halved (from 24k to 12k) but this is similar to that in Cisco Nexus 3000 Series switches.
- 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.

Default Settings for Unicast RPF

This table lists the default settings for Unicast RPF parameters.

Table 15: 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 RPF 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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	interface ethernet <i>slot/port</i> 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	exit Example: switch(config-cmap)# exit switch(config)#	Exits class map configuration mode.
Step 5	(Optional) show ip interface ethernet <i>slot/port</i> Example: switch(config)# show ip interface ethernet 2/3	Displays the IP information for an interface.
Step 6	(Optional) show running-config interface ethernet <i>slot/port</i> Example: switch(config)# show running-config interface ethernet 2/3	Displays the configuration for an interface in the running 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.

Configuration Examples for Unicast RPF

The following example shows how to configure loose Unicast RPF 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 RPF for IPv4 packets:

```
interface Ethernet2/2
 ip address 172.23.231.240/23
 ip 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 <i>slot/port</i>	Displays the interface configuration in the running configuration.
show running-config ip [all]	Displays the IPv4 configuration in the running configuration.
show startup-config interface ethernet <i>slot/port</i>	Displays the interface configuration in the startup configuration.
show startup-config ip	Displays the IP configuration in the startup configuration.



CHAPTER 11

Configuring Control Plane Policing

This chapter contains the following sections:

- [Information About CoPP, on page 127](#)
- [Control Plane Protection, on page 128](#)
- [CoPP Policy Templates, on page 130](#)
- [CoPP Class Maps, on page 134](#)
- [Packets Per Second Credit Limit, on page 135](#)
- [CoPP and the Management Interface, on page 135](#)
- [Licensing Requirements for CoPP, on page 135](#)
- [Guidelines and Limitations for CoPP, on page 135](#)
- [Upgrade Guidelines for CoPP, on page 137](#)
- [Configuring CoPP, on page 137](#)
- [CoPP Show Commands, on page 140](#)
- [Displaying the CoPP Configuration Status, on page 141](#)
- [Monitoring CoPP, on page 142](#)
- [Clearing the CoPP Statistics, on page 142](#)
- [CoPP Configuration Examples, on page 143](#)
- [Sample CoPP Configuration, on page 145](#)
- [Example: Changing or Reapplying the Default CoPP Policy Using the Setup Utility, on page 148](#)

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. You configure packet classifications and rate controlling policies using class-maps and policy-maps.

The following parameters can be used to classify a packet:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 4 protocol

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.

The policing rate is specified in terms of packets per second (PPS). Each classified flow can be policed individually by specifying a policing rate limit in PPS.

CoPP Policy Templates

When you bring up your Cisco NX-OS device for the first time, the Cisco NX-OS software installs the default `copp-system-policy` to protect the supervisor module from DoS attacks. You can choose the CoPP policy template for your deployment scenario by specifying CoPP policy options from the initial setup utility:

- Default—Layer 2 and Layer 3 policy which provides a good balance of policing between switched and routed traffic bound to CPU.
- Layer 2—Layer 2 policy which gives more preference to the Layer 2 traffic (eg BPDU) bound to the CPU
- Layer 3—Layer 3 policy which gives more preference to the Layer 3 traffic (eg BGP, RIP, OSPF etc) bound to the CPU

If you do not select an option or choose not to execute the setup utility, the Cisco NX-OS software applies the Default policing. Cisco recommends starting with the default policy and later modifying the CoPP policies as required.

The default `copp-system-policy` 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.

You can switch across default, Layer 2 and Layer 3 templates by entering the setup utility again using the `setup` command.

Default CoPP Policy

This policy is applied to the switch by default. It has the classes with police rates that should suit most network installations. You cannot modify this policy template, but you can modify the CoPP configuration on the device. After you run the setup utility and set up the default CoPP policy profile, all modifications that were made to the CoPP policy will be removed.

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ip-options
    police pps 100
  class copp-s-ip-nat
    police pps 100
  class copp-s-ipmcmiss
    police pps 400
  class copp-s-ipmc-g-hit
    police pps 400
  class copp-s-ipmc-rpf-fail-g
```

```
    police pps 400
class copp-s-ipmc-rpf-fail-sg
    police pps 400
class copp-s-dhcpreq
    police pps 300
class copp-s-dhcpresp
    police pps 300
class copp-s-igmp
    police pps 400
class copp-s-routingProto2
    police pps 1300
class copp-s-eigrp
    police pps 200
class copp-s-pimreg
    police pps 200
class copp-s-pimautorp
    police pps 200
class copp-s-routingProtol
    police pps 1000
class copp-s-arp
    police pps 200
class copp-s-ntp
    police pps 1000
class copp-s-bpdu
    police pps 12000
class copp-s-cdp
    police pps 400
class copp-s-lacp
    police pps 400
class copp-s-lldp
    police pps 200
class copp-icmp
    police pps 200
class copp-telnet
    police pps 500
class copp-ssh
    police pps 500
class copp-snmp
    police pps 500
class copp-ntp
    police pps 100
class copp-tacacsradius
    police pps 400
class copp-stftp
    police pps 400
class copp-ftp
    police pps 100
class copp-http
    police pps 100
```

Layer 2 CoPP Policy

You cannot modify this policy template, but you can modify the CoPP configuration on the device. After you run the setup utility and set up the Layer 2 CoPP policy profile, all modifications that were made to the CoPP policy will be removed.

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
```

```
class copp-s-l3destmiss
  police pps 100
class copp-s-glean
  police pps 500
class copp-s-l3mtufail
  police pps 100
class copp-s-ttl1
  police pps 100
class copp-s-ip-options
  police pps 100
class copp-s-ip-nat
  police pps 100
class copp-s-ipmcmiss
  police pps 400
class copp-s-ipmc-g-hit
  police pps 400
class copp-s-ipmc-rpf-fail-g
  police pps 400
class copp-s-ipmc-rpf-fail-sg
  police pps 400
class copp-s-dhcpreq
  police pps 300
class copp-s-dhcpresp
  police pps 300
class copp-s-igmp
  police pps 400
class copp-s-routingProto2
  police pps 1200
class copp-s-eigrp
  police pps 200
class copp-s-pimreg
  police pps 200
class copp-s-pimautorp
  police pps 200
class copp-s-routingProto1
  police pps 900
class copp-s-arp
  police pps 200
class copp-s-ptp
  police pps 1000
class copp-s-bpdu
  police pps 12300
class copp-s-cdp
  police pps 400
class copp-s-lacp
  police pps 400
class copp-s-lldp
  police pps 200
class copp-icmp
  police pps 200
class copp-telnet
  police pps 500
class copp-ssh
  police pps 500
class copp-snmp
  police pps 500
class copp-ntp
  police pps 100
class copp-tacacsradius
  police pps 400
class copp-stftp
  police pps 400
class copp-ftp
  police pps 100
```



```
class copp-http
  police pps 100
```

Layer 3 CoPP Policy

You cannot modify this policy template, but you can modify the CoPP configuration on the device. After you run the setup utility and set up the Layer 3 CoPP policy profile, all modifications that were made to the CoPP policy will be removed.

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ip-options
    police pps 100
  class copp-s-ip-nat
    police pps 100
  class copp-s-ipmcmis
    police pps 400
  class copp-s-ipmc-g-hit
    police pps 400
  class copp-s-ipmc-rpf-fail-g
    police pps 400
  class copp-s-ipmc-rpf-fail-sg
    police pps 400
  class copp-s-dhcpreq
    police pps 300
  class copp-s-dhcpresp
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-routingProto2
    police pps 4000
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
    police pps 200
  class copp-s-pimautorp
    police pps 200
  class copp-s-routingProto1
    police pps 4000
  class copp-s-arp
    police pps 200
  class copp-s-ptp
    police pps 1000
  class copp-s-bpdu
    police pps 6000
  class copp-s-cdp
    police pps 200
  class copp-s-lacp
    police pps 200
```

```

class copp-s-lldp
  police pps 200
class copp-icmp
  police pps 200
class copp-telnet
  police pps 500
class copp-ssh
  police pps 500
class copp-snmp
  police pps 500
class copp-ntp
  police pps 100
class copp-tacacsradius
  police pps 400
class copp-stftp
  police pps 400
class copp-ftp
  police pps 100
class copp-http
  police pps 100

```

CoPP Class Maps

Classes within a policy are of two types:

- **Static**—These classes are part of every policy template and cannot be removed from the policy or CoPP configuration. Static classes would typically contain the traffic which is deemed critical to device operation and is required in the policy.
- **Dynamic**—These classes can be created, added or removed from a policy. Using dynamic classes, you can create classes/policing for CPU bound traffic (unicast) specific to their requirements.



Note Classes with names copp-s-x are static classes.

ACLs can be associated with both static and dynamic classes.

Beginning with Cisco NX-OS Release 6.0(2)A8(9), a new CoPP class "copp-s-pim-datareg" is added to match Protocol-Independent Multicast (PIM) data register packets destined to the switch. This CoPP class help classify PIM data register packets to a separate queue, with a policer rate of 600 Packets-Per-Second (pps). To configure the new CoPP classes, you must run the set up script after upgrading to Cisco NX-OS Release 6.0(2)A8(9). The following are the three CoPP classes for the PIM protocol:

- **copp-s-pimreg** - Matches PIM protocol packets which are multicast packets such as PIM hello, join-prune etc.
- **copp-s-pimautorp** – Matches PIM RP election protocol packets.
- **copp-s-pim-datareg** - Matches PIM data register packets.

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).

CoPP and the Management Interface

The Cisco NX-OS device supports only hardware-based CoPP which does not support the management interface (mgmt0). The out-of-band mgmt0 interface connects directly to the CPU and does not pass through the in-band traffic hardware where CoPP is implemented.

On the mgmt0 interface, ACLs can be configured to give or deny access to a particular type of traffic.

Licensing Requirements for CoPP

This feature does not require a license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Guidelines and Limitations for CoPP

CoPP has the following configuration guidelines and limitations:

- Cisco recommends that you choose the default, L2, or L3 policy, depending upon your deployment scenario and later modify the CoPP policies based on observed behavior.
- If you observe +/- 2-5% irregularity in the traffic around 30-40s after the traffic has fully converged after fast-reload, use a higher CoPP value for the ARP packets.
- 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.
- The default police packets per second (PPS) value is changed to 900 for **copp-s-bfd** command with **write erase** command and reload for 6.0(2)U6(1) release.
- Cisco recommends that you continuously monitor CoPP. If drops occur, determine if CoPP dropped traffic unintentionally or in response to a malfunction or attack. In either event, analyze the situation and evaluate the need to use a different CoPP policy or modify the customized CoPP policy.
- The Cisco NX-OS software does not support egress CoPP or silent mode. CoPP is supported only on ingress (**service-policy output copp** cannot be applied to the control plane interface).
- The creation of new CoPP policies is not supported.
- There are no hardware counters for glean, class-default class-map in cache mode.

- There are no hardware counters for class-default in normal mode.
- There are no counters for the MTU fail class-map.
- There are no hardware counters for NAT.
- There are no hardware counters for l3destmiss.
- There are no hardware counters for TTL1.
- There are no hardware counter for IPMCMISS.
- There are no hardware counters for copp-s-ipmc-g-hit, copp-s-ipmc-rpf-fail-g, and copp-s-ipmc-rpf-fail-sg.
- You cannot add match acl statements to a static class-map.
- Starting with Release 6.0(2)U5(1), Cisco Nexus 3000 Series switches drop all the packets when the tunnel is not configured. The packets are also dropped when the tunnel is configured but the tunnel interface is not configured or the tunnel interface is in shut down state.

Point to Point tunnel (Source and Destination) – Cisco Nexus 3000 Series switches decapsulate all IP-in-IP packets destined to it when the command **feature tunnel** is configured and there is an operational tunnel interface configured with the tunnel source and the destination address that matches the incoming packets' outer source and destination addresses. If there is not a source and destination packet match or if the interface is in shutdown state, the packet is dropped.

Decapsulate Tunnel (Source only) - Cisco Nexus 3000 Series switches decapsulate all IP-in-IP packets destined to it when the command **feature tunnel** is configured and there is an operational tunnel interface configured with the tunnel source address that matches the incoming packets' outer destination addresses. If there is not a source packet match or if the interface is in shutdown state, the packet is dropped.

- If you use NXAPI over the front panel port, you must increase the CoPP policy (for http) to allow 3000 PPS traffic so that there is no packet drop and the CLIs with a larger output return within the expected time.
- When you execute the setup script you will be prompted with *Enter to basic configuration (yes/no)?*.
 - If you answer *no*, then the default CoPP policy template will not be applied to the system.
 - If you answer *yes*, then the default CoPP policy template of the running version will be applied to the system. This action will overwrite the non-default policer rates configured on system CoPP classes.



Note If you press CTRL+C during the setup script execution of the script, default CoPP policy template will not be applied into the system and there will be no changes in the existing CoPP policy.

- If you press CTRL+C after executing the setup script and entering into basic configuration, it skips all the remaining steps and you will be prompted to *Apply and save the config before exiting (yes/no)?*.
 - If you answer *no*, then the default CoPP policy template will not be applied to the system.
 - If you answer *yes*, then the default CoPP policy template of the running version is applied. This action will overwrite the non-default policer rates configured on system CoPP classes.

- The setup script will not alter any user defined CoPP classes.
- When a default CoPP policy template is applied as part of successful setup script execution, the control packets may be dropped for a brief period of time. During this window, control plane protocols may flap.
- The setup script may fail to configure the default CoPP policy template when PPS credits are exhausted. This may result in one or more system CoPP classes with zero PPS. This may happen, when there are user defined classes with high PPS values. To apply the default CoPP policy, you must reconfigure the PPS values of user defined CoPP classes and run the setup script once again.
- Hardware and software match packet counters for CDP (copp-s-cdp), LLDP (copp-s-lldp), LACP (copp-s-lacp), BPDU (copp-s-bpdu) classes are aggregated on Cisco Nexus 3548 platform switches. Likewise, hardware and software match packet counters for copp-s-dhcpreq and copp-s-dhcpresp classes are aggregated.

Upgrade Guidelines for CoPP

CoPP has the following upgrade guidelines:

- If you upgrade from a Cisco NX-OS release that does not support the CoPP feature to a release that supports the CoPP feature, CoPP is automatically enabled with the default policy when the switch boots up. You must run the setup script after the upgrade to enable a different policy (default, 13, ,12). Not configuring CoPP protection can leave your NX-OS device vulnerable to DoS attacks.
- If you upgrade from a Cisco NX-OS release that supports the CoPP feature to a Cisco NX-OS release that supports the CoPP feature with additional classes for new protocols, you must run the setup utility for the new CoPP classes to be available.
- Because the setup script modifies the policing rates corresponding to different flows coming into the CPU, we recommend that you run the setup script during a scheduled maintenance period and not during a time when there is traffic on the device.
- When upgrading to Cisco NX-OS Release 6.0(2)A3(1), check whether the default LLDP CoPP value is less than 500 pps. If it is less than 500, manually change it to 500 by using the following commands:

```
switch(config)# policy-map type control-plane copp-system-policy
switch(config-pmap)# class copp-s-lldp
switch(config-pmap-c)# police pps 500
```

Configuring 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.

Before you begin

Ensure that you have configured the IP ACLs if you want to use ACE hit counters in the class maps.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	class-map type control-plane match-any <i>class-map-name</i> Example: switch(config)# class-map type control-plane ClassMapA switch(config-cmap)#	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) match access-group name <i>access-list-name</i> Example: switch(config-cmap)# match access-group name MyAccessList	Specifies matching for an IP ACL. You can repeat this step to match more than one IP ACL. Note The permit and deny ACL keywords are ignored in the CoPP matching.
Step 4	exit Example: switch(config-cmap)# exit switch(config)#	Exits class map configuration mode.
Step 5	(Optional) show class-map type control-plane <i>[class-map-name]</i> Example: switch(config)# show class-map type control-plane	Displays the control plane class map 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 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 PPS for that class is 0.

You can configure policies for IPv4 packets.

Before you begin

Ensure that you have configured a control plane class map.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	policy-map type control-plane <i>policy-map-name</i> Example: <pre>switch(config)# policy-map type control-plane copp-system-policy switch(config-pmap)#</pre>	Specifies a control plane policy map and enters the policy map configuration mode. The policy map name is case sensitive. Note The name of the policy-map cannot be changed. You can only use the copp-system-policy name for the policy-map. The system allows only a single type control-plane policy-map to be configured.
Step 3	class { <i>class-map-name</i> class } Example: <pre>switch(config-pmap)# class ClassMapA switch(config-pmap-c)#</pre>	Specifies a control plane class map name or the class default and enters control plane class configuration mode.
Step 4	police [pps] { <i>pps-value</i> } [bc] <i>burst-size</i> [bytes kbytes mbytes ms packets us] Example: <pre>switch(config-pmap-c)# police pps 100 bc 10</pre>	Specifies the rate limit in terms of packets per second (PPS) and the committed burst (BC). The PPS range is 0 - 20,000. The default PPS is 0. The BC range is from 0 to 512000000. The default BC size unit is bytes.
Step 5	exit Example: <pre>switch(config-pmap-c)# exit switch(config-pmap)#</pre>	Exits policy map class configuration mode.
Step 6	exit Example: <pre>switch(config-pmap)# exit switch(config)#</pre>	Exits policy map configuration mode.
Step 7	(Optional) show policy-map type control-plane [expand] [name <i>class-map-name</i>] Example: <pre>switch(config)# show policy-map type control-plane</pre>	Displays the control plane policy map configuration.

	Command or Action	Purpose
Step 8	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Configuring the Control Plane Service Policy

Before you begin

Configure a control plane policy map.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	control-plane Example: switch(config) # control-plane switch(config-cp) #	Enters control plane configuration mode.
Step 3	exit Example: switch(config-cp) # exit switch(config) #	Exits control plane configuration mode.
Step 4	(Optional) show running-config copp [all] Example: switch(config)# show running-config copp	Displays the CoPP configuration.
Step 5	(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.

CoPP Show Commands

To display CoPP configuration information, enter one of the following show commands:

Command	Purpose
<code>show ip access-lists [acl-name]</code>	Displays all IPv4 ACLs configured in the system, including the CoPP ACLs.
<code>show class-map type control-plane [class-map-name]</code>	Displays the control plane class map configuration, including the ACLs that are bound to this class map.
<code>show policy-map type control-plane [expand] [name policy-map-name]</code>	Displays the control plane policy map with associated class maps and PPS values.
<code>show running-config copp [all]</code>	Displays the CoPP configuration in the running configuration.
<code>show running-config aclmgr [all]</code>	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.
<code>show startup-config copp [all]</code>	Displays the CoPP configuration in the startup configuration.
<code>show startup-config aclmgr [all]</code>	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.

Displaying the CoPP Configuration Status

Procedure

	Command or Action	Purpose
Step 1	<code>switch# show copp status</code>	Displays the configuration status for the CoPP feature.

Example

This example shows how to display the CoPP configuration status:

```
switch# show copp status
```

Monitoring CoPP

Procedure

	Command or Action	Purpose
Step 1	switch# show policy-map interface control-plane	Displays packet-level statistics for all classes that are part of the applied CoPP policy.

Example

This example shows how to monitor CoPP:

```
switch# show policy-map interface control-plane
Control Plane

service-policy input: copp-system-policy

  class-map copp-s-default (match-any)
    police pps 400 , bc 0 packets
      HW Matched Packets  0
      SW Matched Packets  0
  class-map copp-s-ping (match-any)
    match access-group name copp-system-acl-ping
    police pps 100 , bc 0 packets
      HW Matched Packets  0
      SW Matched Packets  0
  ....

switch# show policy-map interface control-plane
Control Plane

service-policy input: copp-system-policy
class-map copp-s-selfIp (match-any)
  police pps 500
  OutPackets 268
  DropPackets 0
```

Clearing the CoPP Statistics

Procedure

	Command or Action	Purpose
Step 1	(Optional) switch# show policy-map interface control-plane	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
```

CoPP Configuration Examples

Creating an IP ACL

```
ip access-list copp-sample-acl
permit udp any any eq 3333
permit udp any any eq 4444
```

The following example shows how to modify the CoPP Policy to drop all IP-in-IP (Protocol 4) packets immediately if there is not an operational tunnel that matches the incoming packet. Create copp-s-ipinip before the default copp-s-selfip policy as displayed in the following example.

```
ip access-list copp-s-ipinip
10 permit 4 any any
class-map type control-plane match-any copp-s-ipinip
match access-group name copp-s-ipinip
policy-map type control-plane copp-system-policy
class copp-s-ipinip
police pps 0
class copp-s-selfip
police pps 500
class copp-s-default
police pps 400
```

Creating a Sample CoPP Class with an Associated IP ACL

The following example shows how to create a new CoPP class and associated ACL:

```
class-map type control-plane copp-sample-class
match access-group name copp-sample-acl
```

The following example shows how to add a class to a CoPP policy:

```
policy-map type control-plane copp-system-policy
Class copp-sample-class
Police pps 100
```

The following example shows how to modify the PPS for an existing class (copp-s-bpdu):

```
policy-map type control-plane copp-system-policy
Class copp-s-bpdu
Police pps <new_pps_value>
```

Associating an ACL with an Existing or New CoPP Class

The following example shows how to associate an ACL with an existing or new CoPP class:

```
class-map type control-plane copp-s-eigrp
match access-grp name copp-system-acl-eigrp6
```

Adding a Class to a CoPP Policy

The following example shows how to add a class to a CoPP policy, if the class has not already been added:

```
policy-map type control-plane copp-system-policy
class copp-s-eigrp
police pps 100
```

Creating an ARP ACL-Based Dynamic Class

ARP ACLs use ARP TCAM. The default size of this TCAM is 0. Before ARP ACLs can be used with CoPP, this TCAM needs to be carved for a non-zero size.

```
hardware profile tcam region arpacl 128
copy running-config startup-config
reload
```

Creating an ARP ACL

```
arp access-list copp-arp-acl
permit ip 20.1.1.1 255.255.255.0 mac any
```

The procedure to associate an ARP ACLs with a class, and adding that class to the CoPP policy, is the same as the procedure for IP ACLs.

Creating a CoPP Class and Associating an ARP ACL

```
class-map type control-plane copp-sample-class
match access-group name copp-arp-acl
```

Removing a Class from a CoPP Policy

```
policy-map type control-plane copp-system-policy
no class-abc
```

Removing a Class from the System

```
no class-map type control-plane copp-abc
```

Displaying the control plane class map configuration

```
show class-map type control-plane copp-s-pim-datareg
class-map type control-plane match-any copp-s-pim-datareg
```

The following example shows the interface control plane information of the copp-s-pim-datareg class:

```
switch# sh policy-map interface control-plane class copp-s-pim-datareg

Control Plane

service-policy input: copp-system-policy

class-map copp-s-pim-datareg (match-any)
  police pps 600 , bc 0 packets
    HW Matched Packets    55753
    SW Matched Packets    33931

switch#
```

Using the insert-before option to see if a packet matches multiple classes and the priority needs to be assigned to one of them

```
policy-map type control-plan copp-system-policy
class copp-ping insert-before copp-icmp
```

Sample CoPP Configuration

The following example shows a sample CoPP configuration with ACLs, classes, policies, and individual class policing:

```
IP access list copp-system-acl-eigrp
  10 permit eigrp any 224.0.0.10/32
IP access list copp-system-acl-icmp
  10 permit icmp any any
IP access list copp-system-acl-igmp
  10 permit igmp any any
IP access list copp-system-acl-ntp
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
IP access list copp-system-acl-pimreg
  10 permit pim any any
IP access list copp-system-acl-ping
  10 permit icmp any any echo
  20 permit icmp any any echo-reply
IP access list copp-system-acl-routingproto1
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
  30 permit udp any 224.0.0.0/24 eq rip
  40 permit tcp any gt 1024 any eq 639
  50 permit tcp any eq 639 any gt 1024
  70 permit ospf any any
  80 permit ospf any 224.0.0.5/32
  90 permit ospf any 224.0.0.6/32
IP access list copp-system-acl-routingproto2
  10 permit udp any 224.0.0.0/24 eq 1985
  20 permit 112 any 224.0.0.0/24
IP access list copp-system-acl-snmp
  10 permit udp any any eq snmp
  20 permit udp any any eq snmptrap
IP access list copp-system-acl-ssh
  10 permit tcp any any eq 22
  20 permit tcp any eq 22 any
IP access list copp-system-acl-stftp
  10 permit udp any any eq tftp
  20 permit udp any any eq 1758
  30 permit udp any eq tftp any
  40 permit udp any eq 1758 any
  50 permit tcp any any eq 115
  60 permit tcp any eq 115 any
IP access list copp-system-acl-tacacsradius
  10 permit tcp any any eq tacacs
  20 permit tcp any eq tacacs any
  30 permit udp any any eq 1812
  40 permit udp any any eq 1813
  50 permit udp any any eq 1645
  60 permit udp any any eq 1646
  70 permit udp any eq 1812 any
  80 permit udp any eq 1813 any
  90 permit udp any eq 1645 any
  100 permit udp any eq 1646 any
```

```

IP access list copp-system-acl-telnet
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any eq telnet any
  40 permit tcp any eq 107 any
IP access list copp-system-dhcp-relay
  10 permit udp any eq bootps any eq bootps
IP access list test
  statistics per-entry
  10 permit ip 1.2.3.4/32 5.6.7.8/32 [match=0]
  20 permit udp 11.22.33.44/32 any [match=0]
  30 deny udp 1.1.1.1/32 any [match=0]

class-map type control-plane match-any copp-icmp
  match access-group name copp-system-acl-icmp
class-map type control-plane match-any copp-ntp
  match access-group name copp-system-acl-ntp
class-map type control-plane match-any copp-s-arp
class-map type control-plane match-any copp-s-bfd
class-map type control-plane match-any copp-s-bpdu
class-map type control-plane match-any copp-s-dai
class-map type control-plane match-any copp-s-default
class-map type control-plane match-any copp-s-dhcpreq
  match access-group name copp-system-acl-dhcps6
class-map type control-plane match-any copp-s-dhcpresp
  match access-group name copp-system-acl-dhcpc6
  match access-group name copp-system-dhcp-relay
class-map type control-plane match-any copp-s-eigrp
  match access-group name copp-system-acl-eigrp
  match access-group name copp-system-acl-eigrp6
class-map type control-plane match-any copp-s-glean
class-map type control-plane match-any copp-s-igmp
  match access-group name copp-system-acl-igmp
class-map type control-plane match-any copp-s-ipmcmis
class-map type control-plane match-any copp-s-l2switched
class-map type control-plane match-any copp-s-l3destmiss
class-map type control-plane match-any copp-s-l3mtufail
class-map type control-plane match-any copp-s-l3slowpath
class-map type control-plane match-any copp-s-pimautorp
class-map type control-plane match-any copp-s-pimreg
  match access-group name copp-system-acl-pimreg
class-map type control-plane match-any copp-s-ping
  match access-group name copp-system-acl-ping
class-map type control-plane match-any copp-s-ntp
class-map type control-plane match-any copp-s-routingProto1
  match access-group name copp-system-acl-routingproto1
  match access-group name copp-system-acl-v6routingproto1
class-map type control-plane match-any copp-s-routingProto2
  match access-group name copp-system-acl-routingproto2
class-map type control-plane match-any copp-s-selfIp
class-map type control-plane match-any copp-s-ttl1
class-map type control-plane match-any copp-s-v6routingProto2
  match access-group name copp-system-acl-v6routingProto2
class-map type control-plane match-any copp-s-nmp
  match access-group name copp-system-acl-snm
class-map type control-plane match-any copp-s-sh
  match access-group name copp-system-acl-ssh
class-map type control-plane match-any copp-s-tftp
  match access-group name copp-system-acl-stftp
class-map type control-plane match-any copp-s-tacacsradius
  match access-group name copp-system-acl-tacacsradius
class-map type control-plane match-any copp-telnet
  match access-group name copp-system-acl-telnet

```

```
policy-map type control-plane copp-system-policy
  class copp-s-selfIp
    police pps 500
  class copp-s-default
    police pps 400
  class copp-s-l2switched
    police pps 200
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ipmcmis
    police pps 400
  class copp-s-l3slowpath
    police pps 100
  class copp-s-dhcpreq
    police pps 300
  class copp-s-dhcpresp
    police pps 300
  class copp-s-dai
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-routingProto2
    police pps 1300
  class copp-s-v6routingProto2
    police pps 1300
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
    police pps 200
  class copp-s-pimautorp
    police pps 200
  class copp-s-routingProto1
    police pps 1000
  class copp-s-arp
    police pps 200
  class copp-s-ptp
    police pps 1000
  class copp-s-bfd
    police pps 350
  class copp-s-bpdu
    police pps 12000
  class copp-icmp
    police pps 200
  class copp-telnet
    police pps 500
  class copp-ssh
    police pps 500
  class copp-snmp
    police pps 500
  class copp-ntp
    police pps 100
  class copp-tacacsradius
    police pps 400
  class copp-stftp
    police pps 400
```

```
control-plane
service-policy input copp-system-policy
```

Example: 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:

```
switch# setup

----- Basic System Configuration Dialog -----

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

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 : switch

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: n

Configure the default gateway for mgmt? (yes/no) [y]: n

Enable the telnet service? (yes/no) [n]: y

Enable the ssh service? (yes/no) [y]: n

Configure the ntp server? (yes/no) [n]: n

Configure CoPP System Policy Profile ( default / 12 / 13 ) [default]: 12

The following configuration will be applied:
switchname switch
telnet server enable
no ssh server enable
policy-map type control-plane copp-system-policy ( 12 )

Would you like to edit the configuration? (yes/no) [n]: n

Use this configuration and save it? (yes/no) [y]: y

[#####] 100%
```




INDEX

A

- AAA [3, 5, 6, 7, 9, 14, 17, 18, 29](#)
 - accounting [5](#)
 - authentication [5](#)
 - benefits [6](#)
 - configuring console login [9](#)
 - configuring for RADIUS servers [29](#)
 - default settings [18](#)
 - description [3](#)
 - enabling MSCHAP authentication [14](#)
 - example configuration [17](#)
 - guidelines [9](#)
 - limitations [9](#)
 - prerequisites [9](#)
 - user login process [7](#)
 - verifying configurations [17](#)
- AAA accounting [14](#)
 - configuring default methods [14](#)
- AAA accounting logs [17](#)
 - clearing [17](#)
 - displaying [17](#)
- AAA authorization [44](#)
 - configuring on TACACS+ servers [44](#)
- AAA logins [11](#)
 - enabling authentication failure messages [11](#)
- AAA protocols [5](#)
 - RADIUS [5](#)
 - TACACS+ [5](#)
- AAA server groups [6](#)
 - description [6](#)
- AAA servers [14, 16](#)
 - specifying SNMPv3 parameters [14, 16](#)
 - specifying user roles [16](#)
 - specifying user roles in VSAs [14](#)
- AAA services [6](#)
 - configuration options [6](#)
 - remote [6](#)
- accounting [5](#)
 - description [5](#)
- ACL [68, 70](#)
 - processing order [68](#)
 - sequence numbers [70](#)
- ACL implicit rules [69](#)

- ACL TCAM regions [83, 86](#)
 - configuring [83](#)
 - reverting to default sizes [86](#)
- ACLs [67, 69, 72, 80](#)
 - applications [67](#)
 - guidelines [72](#)
 - identifying traffic by protocols [69](#)
 - licensing [72](#)
 - limitations [72](#)
 - prerequisites [72](#)
 - types [67](#)
 - VLAN [80](#)
- authentication [5, 6, 7](#)
 - description [5](#)
 - local [5](#)
 - methods [6](#)
 - remote [5](#)
 - user login [7](#)
- authorization [7, 46](#)
 - user login [7](#)
 - verifying commands [46](#)

C

- changed information [1](#)
 - description [1](#)
- Cisco [16, 21](#)
 - vendor ID [16, 21](#)
- cisco-av-pair [14, 16](#)
 - specifying AAA user parameters [14, 16](#)
- class maps [134, 137](#)
 - configuring for CoPP [137](#)
 - CoPP [134](#)
- clearing statistics [142](#)
 - CoPP [142](#)
- commands [46](#)
 - disabling authorization verification [46](#)
 - enabling authorization verification [46](#)
- configuration example [145](#)
- configuration examples [143](#)
 - CoPP [143](#)
- configuration status [141](#)
 - CoPP [141](#)
- control plane class maps [140](#)
 - verifying the configuration [140](#)

- control plane policy maps [140](#)
 - verifying the configuration [140](#)
- control plane protection [128, 129](#)
 - CoPP [128](#)
 - packet types [129](#)
- control plane protection, classification [129](#)
- control plane protection, CoPP [129](#)
 - rate controlling mechanisms [129](#)
- control plane service policy, configuring [140](#)
 - CoPP [140](#)
- CoPP [127, 128, 129, 130, 134, 135, 137, 138, 140, 141, 142, 143](#)
 - class maps [134](#)
 - clearing statistics [142](#)
 - configuration examples [143](#)
 - configuration status [141](#)
 - configuring class maps [137](#)
 - configuring policy maps [138](#)
 - control plane protection [128](#)
 - control plane protection, classification [129](#)
 - control plane service policy, configuring [140](#)
 - default policy [130](#)
 - guidelines [135](#)
 - information about [127](#)
 - licensing [135](#)
 - limitations [135](#)
 - monitoring [142](#)
 - policy templates [130](#)
 - restrictions for management interfaces [135](#)
 - upgrade guidelines [137](#)
 - verifying the configuration [140](#)
- CoPP policy [131](#)
 - layer 2 [131](#)
- CoPP policy maps [138](#)
 - configuring [138](#)

D

- default CoPP policy [130](#)
- default settings [18, 112](#)
 - AAA [18](#)
 - MAC ACLs [112](#)
- denial-of-service attacks [122](#)
 - IP address spoofing, mitigating [122](#)
- DHCP binding database [93](#)
- DHCP Option 82 [98, 99](#)
 - enabling or disabling data insertion and removal [98, 99](#)
- DHCP relay agent [93, 102, 103, 104](#)
 - described [93](#)
 - enabling or disabling [102](#)
 - enabling or disabling Option 82 [102](#)
 - enabling or disabling subnet broadcast support on a Layer 3 Interface [104](#)
 - enabling or disabling VRF support [103](#)
 - VRF support [93](#)
- DHCP relay binding database [94](#)
 - description [94](#)

- DHCP relay statistics [110](#)
 - clearing [110](#)
- DHCP server addresses [105](#)
 - configuring [105](#)
- dhcp snooping [94](#)
 - licensing [94](#)
 - prerequisites [94](#)
- DHCP snooping [91, 93, 95](#)
 - binding database [93](#)
 - default settings [95](#)
 - guidelines [95](#)
 - limitations [95](#)
 - overview [91](#)
- DHCP snooping binding database [93](#)
 - described [93](#)
 - description [93](#)
 - entries [93](#)
- DoS attacks [122](#)
 - Unicast RPF, deploying [122](#)

E

- examples [18](#)
 - AAA configurations [18](#)

G

- guidelines [72, 95, 135](#)
 - ACLs [72](#)
 - CoPP [135](#)
 - DHCP snooping [95](#)

I

- IDs [16, 21](#)
 - Cisco vendor ID [16, 21](#)
- IP ACL [74](#)
 - creating [74](#)
- IP ACL implicit rules [69](#)
- IP ACL statistics [79](#)
 - clearing [79](#)
 - monitoring [79](#)
- IP ACLs [4, 67, 70, 74, 75, 76, 77, 78](#)
 - applications [67](#)
 - applying as a Router ACL [78](#)
 - applying as port ACLs [77](#)
 - changing [74](#)
 - changing sequence numbers in [76](#)
 - description [4](#)
 - logical operation units [70](#)
 - logical operators [70](#)
 - removing [75](#)
 - types [67](#)

L

- layer 2 [131](#)
 - CoPP policy [131](#)
- licensing [72, 94, 122, 135](#)
 - ACLs [72](#)
 - CoPP [135](#)
 - dhcp snooping [94](#)
 - Unicast RPF [122](#)
- limitations [72, 95, 135](#)
 - ACLs [72](#)
 - CoPP [135](#)
 - DHCP snooping [95](#)
- logical operation units [70](#)
 - IP ACLs [70](#)
- logical operators [70](#)
 - IP ACLs [70](#)
- login [27](#)
 - RADIUS servers [27](#)
- LOU, *See* logical operation units

M

- MAC ACL implicit rules [69](#)
- MAC ACLs [111, 112](#)
 - default settings [112](#)
 - description [111](#)
- MAC packet classification [111, 118](#)
 - configuring [118](#)
 - description [111](#)
- management interfaces [135](#)
 - CoPP restrictions [135](#)
- monitoring [20, 30, 142](#)
 - CoPP [142](#)
 - RADIUS [20](#)
 - RADIUS servers [30](#)
- MSCHAP [14](#)
 - enabling authentication [14](#)

N

- new information [1](#)
 - description [1](#)

P

- policy templates [130](#)
 - description [130](#)
- port ACL [77](#)
- prerequisites [94](#)
 - dhcp snooping [94](#)
- preshared keys [36](#)
 - TACACS+ [36](#)
- privilege level support for TACACS+ authorization [47](#)
 - configuring [47](#)

- privilege roles [49](#)
 - permitting or denying commands for [49](#)

R

- RADIUS [4, 19, 20, 22, 28, 33, 34](#)
 - configuring servers [22](#)
 - configuring timeout intervals [28](#)
 - configuring transmission retry counts [28](#)
 - default settings [34](#)
 - description [4](#)
 - example configurations [33](#)
 - monitoring [20](#)
 - network environments [19](#)
 - operations [20](#)
 - prerequisites [22](#)
 - statistics, displaying [33](#)
- RADIUS server groups [26](#)
 - global source interfaces [26](#)
- RADIUS server preshared keys [24](#)
- RADIUS servers [27, 29, 32, 33](#)
 - allowing users to specify at login [27](#)
 - configuring AAA for [29](#)
 - configuring timeout interval [29](#)
 - configuring transmission retry count [29](#)
 - deleting hosts [32](#)
 - displaying statistics [33](#)
 - example configurations [33](#)
 - manually monitoring [32](#)
- RADIUS statistics [33](#)
 - clearing [33](#)
- RADIUS, global preshared keys [23](#)
- RADIUS, periodic server monitoring [30](#)
- RADIUS, server hosts [23](#)
 - configuring [23](#)
- rate controlling mechanisms [129](#)
 - control plane protection, CoPP [129](#)
- remote devices [61](#)
 - connecting to using SSH [61](#)
- router ACLs [78](#)
- rules [69](#)
 - implicit [69](#)

S

- sample configuration [145](#)
- server groups [6](#)
- servers [27](#)
 - RADIUS [27](#)
- SNMPv3 [14, 16](#)
 - specifying AAA parameters [14](#)
 - specifying parameters for AAA servers [16](#)
- source interfaces [26, 42](#)
 - RADIUS server groups [26](#)
 - TACACS+ server groups [42](#)

SSH 4

- description 4

- SSH clients 57

- SSH server keys 57

- SSH servers 57

- SSH sessions 61, 62

- clearing 62

- connecting to remote devices 61

- statistics 54, 79

- clearing 79

- monitoring 79

- TACACS+ 54

T

- TACACS+ 4, 35, 36, 37, 38, 46, 50, 54, 55

- advantages over RADIUS 35

- configuring 38

- configuring global timeout interval 50

- description 4, 35

- displaying statistics 54

- example configurations 55

- field descriptions 55

- global preshared keys 36

- limitations 38

- prerequisites 37

- preshared key 36

- user login operation 36

- verifying command authorization 46

- verifying configuration 54

- TACACS+ command authorization 45, 46

- configuring 45

- testing 46

- TACACS+ server groups 42

- global source interfaces 42

- TACACS+ servers 38, 50, 51, 53, 54, 55

- configuring hosts 38

- configuring TCP ports 51

- configuring timeout interval 50

- displaying statistics 54

- field descriptions 55

- manually monitoring 53

- verifying configuration 54

- TCAMs 83, 86

- configuring 83

- reverting to default sizes 86

- TCP ports 51

- TACACS+ servers 51

- Telnet 4

- description 4

- Telnet server 64

- enabling 64

- reenabling 64

- Telnet servers 58

- Telnet sessions 64, 65

- clearing 65

- connecting to remote devices 64

U

- Unicast RPF 121, 122, 123, 124, 125

- BOOTP and 122

- default settings 123

- deploying 122

- description 121, 122

- DHCP and 122

- example configurations 124

- FIB 121

- guidelines 122

- licensing 122

- limitations 122

- loose mode 123

- statistics 122

- strict mode 123

- tunneling and 122

- verifying configuration 125

- upgrade 137

- guidelines for CoPP 137

- user login 7

- authentication process 7

- authorization process 7

- user roles 14, 16

- specifying on AAA servers 14, 16

V

- vendor-specific attributes 16

- VLAN ACLs 80

- information about 80

- VSA's 16

- format 16

- protocol options 16

- support description 16