



## **Cisco Nexus 3000 Series NX-OS Security Configuration Guide, Release 5.0(3)U2(2)**

**First Published:** October 13, 2011

**Last Modified:** December 28, 2011

### **Americas Headquarters**

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

Text Part Number: OL-25780-01

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 NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2011-2012 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### Preface

#### Preface xi

Audience xi

Document Conventions xi

Related Documentation for Nexus 3000 Series NX-OS Software xii

Obtaining Documentation and Submitting a Service Request xiv

---

### 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 5

---

### CHAPTER 3

#### Configuring Authentication, Authorization, and Accounting 7

Information About AAA 7

AAA Security Services 7

Benefits of Using AAA 8

Remote AAA Services 8

AAA Server Groups 9

AAA Service Configuration Options 9

Authentication and Authorization Process for User Login 10

Prerequisites for Remote AAA 11

Information about AAA Guidelines and Limitations 12

Configuring AAA 12

Configuring Console Login Authentication Methods 12

Configuring Default Login Authentication Methods	13
Enabling Login Authentication Failure Messages	15
Configuring AAA Command Authorization	15
Enabling MSCHAP Authentication	17
Configuring AAA Accounting Default Methods	18
Using AAA Server VSAs	20
About VSAs	20
VSA Format	20
Specifying Switch User Roles and SNMPv3 Parameters on AAA Servers	21
Displaying and Clearing the Local AAA Accounting Log	21
Verifying AAA Configuration	22
Example AAA Configuration	22
Default AAA Settings	22

**CHAPTER 4****Configuring RADIUS 25**

Configuring RADIUS	25
Information About RADIUS	25
RADIUS Network Environments	25
RADIUS Operations	26
RADIUS Server Monitoring	26
Vendor-Specific Attributes	27
Prerequisites for RADIUS	28
Guidelines and Limitations for RADIUS	28
Configuring RADIUS Servers	28
Configuring RADIUS Server Hosts	29
Configuring RADIUS Global Preshared Keys	30
Configuring RADIUS Server Preshared Keys	31
Configuring RADIUS Server Groups	32
Configuring the Global Source Interface for RADIUS Server Groups	34
Allowing Users to Specify a RADIUS Server at Login	35
Configuring the Global RADIUS Transmission Retry Count and Timeout Interval	35
Configuring the RADIUS Transmission Retry Count and Timeout Interval for a Server	36
Configuring Accounting and Authentication Attributes for RADIUS Servers	37
Configuring Periodic RADIUS Server Monitoring	39

Configuring the Dead-Time Interval	40
Manually Monitoring RADIUS Servers or Groups	41
Verifying RADIUS Configuration	42
Displaying RADIUS Server Statistics	43
Example RADIUS Configuration	43
Default RADIUS Settings	43

---

**CHAPTER 5****Configuring TACACS+ 45**

About Configuring TACACS+	45
Information About TACACS+	45
TACACS+ Advantages	45
User Login with TACACS+	46
Default TACACS+ Server Encryption Type and Preshared Key	46
Command Authorization Support for TACACS+ Servers	47
TACACS+ Server Monitoring	47
Prerequisites for TACACS+	47
Guidelines and Limitations for TACACS+	48
Configuring TACACS+	48
TACACS+ Server Configuration Process	48
Enabling TACACS+	49
Configuring TACACS+ Server Hosts	49
Configuring TACACS+ Global Preshared Keys	50
Configuring TACACS+ Server Preshared Keys	51
Configuring TACACS+ Server Groups	52
Configuring the Global Source Interface for TACACS+ Server Groups	54
Specifying a TACACS+ Server at Login	55
Configuring AAA Authorization on TACACS+ Servers	56
Configuring Command Authorization on TACACS+ Servers	57
Testing Command Authorization on TACACS+ Servers	59
Enabling and Disabling Command Authorization Verification	59
Configuring Privilege Level Support for Authorization on TACACS+ Servers	60
Permitting or Denying Commands for Users of Privilege Roles	62
Configuring the Global TACACS+ Timeout Interval	63
Configuring the Timeout Interval for a Server	64
Configuring TCP Ports	65

Configuring Periodic TACACS+ Server Monitoring	66
Configuring the Dead-Time Interval	67
Manually Monitoring TACACS+ Servers or Groups	68
Disabling TACACS+	68
Displaying TACACS+ Statistics	69
Verifying TACACS+ Configuration	69
Configuration Examples for TACACS+	70
Default TACACS+ Settings	70

**CHAPTER 6****Configuring SSH and Telnet 73**

Configuring SSH and Telnet	73
Information About SSH and Telnet	73
SSH Server	73
SSH Client	73
SSH Server Keys	73
Telnet Server	74
Guidelines and Limitations for SSH	74
Configuring SSH	74
Generating SSH Server Keys	74
Specifying the SSH Public Keys for User Accounts	75
Specifying the SSH Public Keys in Open SSH Format	75
Specifying the SSH Public Keys in IETF SECSH Format	76
Specifying the SSH Public Keys in PEM-Formatted Public Key Certificate Form	77
Starting SSH Sessions to Remote Devices	78
Clearing SSH Hosts	79
Disabling the SSH Server	79
Deleting SSH Server Keys	80
Clearing SSH Sessions	80
SSH Example Configuration	81
Configuring Telnet	82
Enabling the Telnet Server	82
Reenabling the Telnet Server	82
Starting Telnet Sessions to Remote Devices	83
Clearing Telnet Sessions	83

Verifying the SSH and Telnet Configuration 84  
Default SSH Settings 84

---

**CHAPTER 7****Configuring Access Control Lists 85**

Information About ACLs 85  
IP ACL Types and Applications 85  
    Application Order 86  
Rules 86  
    Source and Destination 86  
    Protocols 86  
    Implicit Rules 87  
    Additional Filtering Options 87  
    Sequence Numbers 87  
    Logical Operators and Logical Operation Units 88  
Configuring IP ACLs 88  
    Creating an IP ACL 88  
    Changing an IP ACL 89  
    Removing an IP ACL 91  
    Changing Sequence Numbers in an IP ACL 91  
    Applying an IP ACL to mgmt0 92  
    Applying an IP ACL as a Port ACL 93  
    Verifying IP ACL Configurations 94  
        Monitoring and Clearing IP ACL Statistics 94  
Information About VLAN ACLs 95  
    VACLs and Access Maps 95  
    VACLs and Actions 95  
    Statistics 95  
Configuring VACLs 96  
    Creating or Changing a VACL 96  
    Removing a VACL 97  
    Applying a VACL to a VLAN 97  
    Verifying VACL Configuration 98  
        Displaying and Clearing VACL Statistics 98  
Configuration Examples for VACL 99  
Configuring ACL TCAM Region Sizes 99

Reverting to the Default TCAM Region Sizes	101
Configuring ACLs on Virtual Terminal Lines	102
Verifying ACLs on VTY Lines	103
Configuration Examples for ACLs on VTY Lines	103
Default ACL Settings	104

**CHAPTER 8****Configuring DHCP Snooping 107**

Information About DHCP Snooping	107
Feature Enabled and Globally Enabled	108
Trusted and Untrusted Sources	108
DHCP Snooping Binding Database	109
Information About the DHCP Relay Agent	109
DHCP Relay Agent	109
VRF Support for the DHCP Relay Agent	110
DHCP Relay Binding Database	110
Guidelines and Limitations for DHCP Snooping	110
Default Settings for DHCP Snooping	111
Configuring DHCP Snooping	111
Minimum DHCP Snooping Configuration	111
Enabling or Disabling the DHCP Snooping Feature	112
Enabling or Disabling DHCP Snooping Globally	113
Enabling or Disabling DHCP Snooping on a VLAN	113
Enabling or Disabling Strict DHCP Packet Validation	114
Configuring an Interface as Trusted or Untrusted	115
Enabling or Disabling the DHCP Relay Agent	117
Enabling or Disabling VRF Support for the DHCP Relay Agent	118
Creating a DHCP Static Binding	119
Verifying the DHCP Snooping Configuration	120
Displaying DHCP Bindings	120
Clearing the DHCP Snooping Binding Database	121
Configuration Examples for DHCP Snooping	122

**CHAPTER 9****Configuring Dynamic ARP Inspection 123**

Information About DAI	123
Understanding ARP	123

Understanding ARP Spoofing Attacks	124
Understanding DAI and ARP Spoofing Attacks	124
Interface Trust States and Network Security	125
Logging DAI Packets	126
Licensing Requirements for DAI	127
Prerequisites for DAI	127
Guidelines and Limitations for DAI	127
Default Settings for DAI	128
Configuring DAI	129
Enabling or Disabling DAI on VLANs	129
Configuring the DAI Trust State of a Layer 2 Interface	130
Enabling or Disabling Additional Validation	131
Configuring the DAI Logging Buffer Size	132
Configuring DAI Log Filtering	133
Verifying the DAI Configuration	134
Monitoring and Clearing DAI Statistics	135
Configuration Examples for DAI	135
Example 1 Two Devices Support DAI	135
Configuring Device A	136
Configuring Device B	138

---

**CHAPTER 10**

<b>Configuring Unicast RPF</b>	<b>141</b>
Information About Unicast RPF	141
Unicast RPF Process	142
Global Statistics	143
Licensing Requirements for Unicast RPF	143
Guidelines and Limitations for Unicast RPF	143
Default Settings for Unicast RPF	144
Configuring Unicast RPF	144
Configuration Examples for Unicast RPF	146
Verifying Unicast RPF Configuration	147

---

**CHAPTER 11**

<b>Configuring Control Plane Policing</b>	<b>149</b>
Information About CoPP	149
Control Plane Protection	151

Control Plane Packet Types	151
Classification	151
Rate Controlling Mechanisms	152
CoPP Policy Templates	152
Default CoPP Policy	152
Layer 2 CoPP Policy	153
Layer 3 CoPP Policy	154
CoPP Class Maps	155
CoPP Configuration Information	156
Packets Per Second Credit Limit	156
CoPP and the Management Interface	156
Licensing Requirements for CoPP	156
Guidelines and Limitations for CoPP	156
Configuring CoPP	157
Configuring a Control Plane Class Map	157
Configuring a Control Plane Policy Map	158
Configuring the Control Plane Service Policy	160
CoPP Show Commands	161
Displaying the CoPP Configuration Status	162
Monitoring CoPP	162
Clearing the CoPP Statistics	163
CoPP Configuration Examples	163
Sample CoPP Configuration	164
Example: Changing or Reapplying the Default CoPP Policy Using the Setup Utility	167
Additional References for CoPP	167
Feature History for CoPP	168



## Preface

---

This preface contains the following sections:

- [Audience, page xi](#)
- [Document Conventions, page xi](#)
- [Related Documentation for Nexus 3000 Series NX-OS Software, page xii](#)
- [Obtaining Documentation and Submitting a Service Request, page xiv](#)

## Audience

This publication is for experienced network administrators who configure and maintain Cisco Nexus Series switches.

## Document Conventions

Command descriptions use the following conventions:

Convention	Description
<b>bold</b>	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.
<b><code>boldface screen font</code></b>	Information you must enter is in boldface screen font.
<i><code>italic screen font</code></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.

## Related Documentation for Nexus 3000 Series NX-OS Software

The entire Cisco NX-OS 3000 Series documentation set is available at the following URL:

[http://www.cisco.com/en/US/products/ps11541/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html)

### Release Notes

The release notes are available at the following URL:

[http://www.cisco.com/en/US/products/ps11541/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html)

### Installation and Upgrade Guides

The installation and upgrade guides are available at the following URL:

[http://www.cisco.com/en/US/products/ps11541/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps11541/prod_installation_guides_list.html)

The documents in this category include:

- *Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series Safety Information and Documentation*
- *Regulatory, Compliance, and Safety Information for the Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series*
- *Cisco Nexus 3000 Series Hardware Installation Guide*

### Configuration Guides

The configuration guides are available at the following URL:

[http://www.cisco.com/en/US/products/ps11541/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps11541/products_installation_and_configuration_guides_list.html)

The documents in this category include:

- *Configuration Limits for Cisco NX-OS*
- *Fundamentals Configuration Guide*
- *Layer 2 Switching Configuration Guide*
- *Multicast Configuration Guide*
- *Quality of Service Configuration Guide*
- *Security Configuration Guide*
- *System Management Configuration Guide*
- *Unicast Routing Configuration Guide*
- *Verified Scalability Guide for Cisco NX-OS*

### Technical References

The technical references are available at the following URL:

[http://www.cisco.com/en/US/products/ps11541/prod\\_technical\\_reference\\_list.html](http://www.cisco.com/en/US/products/ps11541/prod_technical_reference_list.html)

### Error and System Messages

The error and system message reference guides are available at the following URL:

[http://www.cisco.com/en/US/products/ps11541/products\\_system\\_message\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps11541/products_system_message_guides_list.html)

# Obtaining Documentation and Submitting a Service Request

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

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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



# CHAPTER 1

## New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 3000 Series NX-OS Security Configuration Guide*.

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

## New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 3000 Series NX-OS Security Configuration Guide*.

The latest version of this document is available at the following Cisco website:

[http://www.cisco.com/en/US/products/ps11541/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps11541/products_installation_and_configuration_guides_list.html)

To check for the latest information about Cisco NX-OS for the Cisco Nexus 3000 Series switch, see the *Cisco Nexus 3000 Series Release Notes* available at the following Cisco website:

[http://www.cisco.com/en/US/products/ps11541/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html)

**Table 1: New and Changed Security Features for Cisco NX-OS Release 5.0(3)U2(2)**

Feature	Description	Where Documented
Control Plane Policing (CoPP)	Support for Control Plane Policing.	<a href="#">Control Plane Policing</a>
Support for L40p port comparison for egress RACLs	Documentation of restrictions for egress RACLs.	<a href="#">Applying an IP ACL as a Router ACL</a> <a href="#">Information About VLAN ACLs</a>





## CHAPTER 2

# Overview

---

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

- [Authentication, Authorization, and Accounting, page 3](#)
- [RADIUS and TACACS+ Security Protocols, page 4](#)
- [SSH and Telnet, page 4](#)
- [IP ACLs, page 5](#)

## 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.

### Related Topics

[Configuring AAA](#)

## 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.

### Related Topics

[Configuring RADIUS](#)

[Configuring TACACS+, on page 45](#)

## 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.

**Related Topics**

[Configuring SSH and Telnet, on page 73](#)

## 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.

**Related Topics**

[Configuring IP ACLs](#)





## CHAPTER 3

# Configuring Authentication, Authorization, and Accounting

---

This chapter describes how to configure authentication, authorization, and accounting (AAA) on Cisco Nexus 3000 Series switches. It contains the following sections:

- [Information About AAA, page 7](#)
- [Prerequisites for Remote AAA, page 11](#)
- [Information about AAA Guidelines and Limitations, page 12](#)
- [Configuring AAA, page 12](#)
- [Displaying and Clearing the Local AAA Accounting Log , page 21](#)
- [Verifying AAA Configuration, page 22](#)
- [Example AAA Configuration, page 22](#)
- [Default AAA Settings, page 22](#)

## 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 managing Cisco Nexus 3000 Series switches. The Cisco Nexus 3000 Series switches support Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control device Plus (TACACS+) protocols.

Based on the user ID and password combination that you provide, the Cisco Nexus 3000 Series 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.

Authentication is the process of verifying the identity of the person or device accessing the Cisco Nexus 3000 Series switches. This process is based on the user ID and password combination provided by the entity trying to access the switch. The Cisco Nexus 3000 Series switches allow you to perform local authentication (using the local lookup database) or remote authentication (using one or more RADIUS or TACACS+ servers).

- **Authorization**—Provides access control.

AAA authorization is the process of assembling a set of attributes that describe what the user is authorized to perform. Authorization in Cisco Nexus 3000 Series switches is provided by attributes that are downloaded from AAA servers. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user.

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

The accounting feature tracks and maintains a log of every management session used to access the Cisco Nexus 3000 Series switches. You can use this information to generate reports for troubleshooting and auditing purposes. You can store accounting logs locally or send them to remote AAA servers.

**Note**

---

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

---

## 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 Cisco Nexus 3000 Series 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 than using the local databases on the switches are easier to manage.

## AAA Server Groups

You can specify remote AAA servers for authentication, authorization, and accounting using server groups. A server group is a set of remote AAA servers that implement the same AAA protocol. The purpose of a server group is to provide for failover servers in case a remote AAA server fails to respond. If the first remote server in the group fails to respond, the next remote server in the group is tried until one of the servers sends a response. If all the AAA servers in the server group fail to respond, then that server group option is considered a failure. If required, you can specify multiple server groups. If a Cisco Nexus 3000 Series 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 3000 Series switches, 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	<b>aaa authentication login default</b>
Console login	<b>aaa authentication login console</b>
User session accounting	<b>aaa accounting default</b>

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 user name.



### Note

If the method is for all RADIUS servers, instead of a specific server group, the Cisco Nexus 3000 Series switches 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 Nexus 5000 Series switches.

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 3000 Series switches try each option in the order specified. The local option is the default method when other configured options fail.

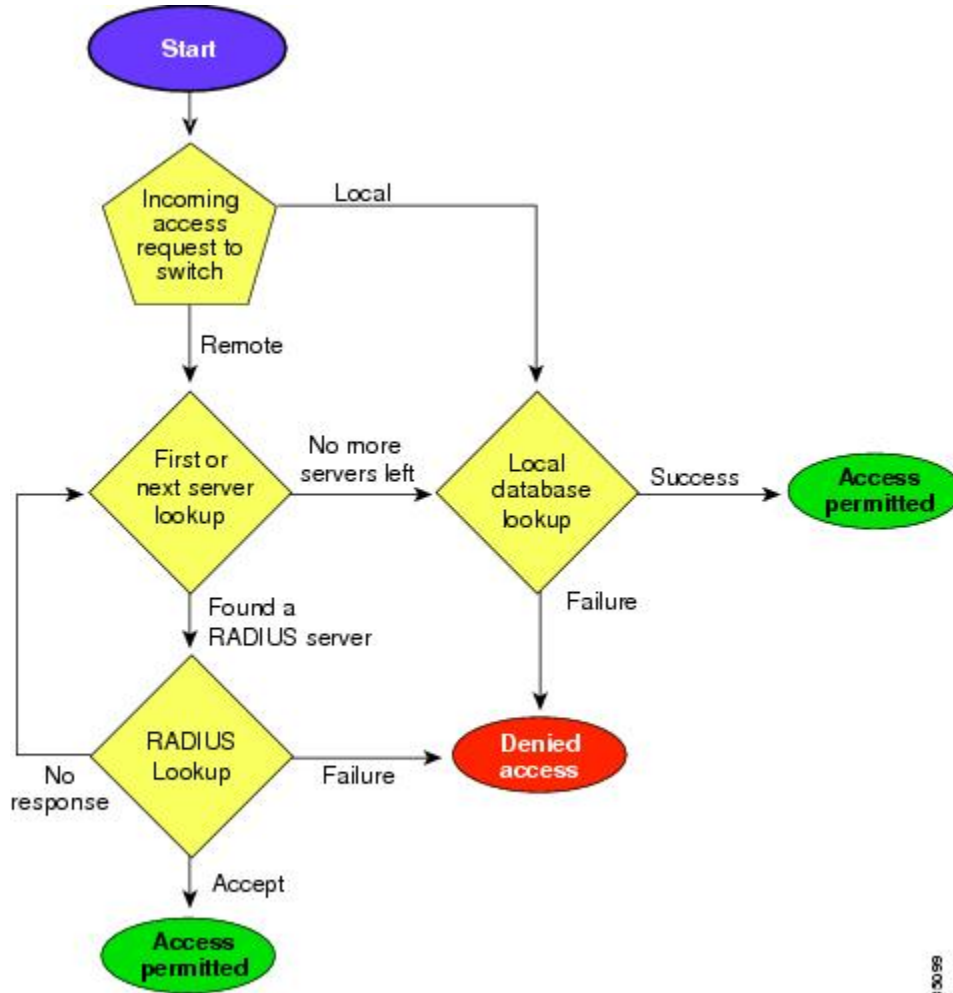
## Authentication and Authorization Process for User Login

The figure below shows a flowchart of the authentication and authorization process for user login. The following process occurs:

- When you log in to the required Cisco Nexus 3000 Series switch, 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 3000 Series switch 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, then the servers in the next server group are tried.
  - If all configured methods fail, then the local database is used for authentication.
- If the Cisco Nexus 3000 Series switches successfully authenticate you through a remote AAA server, then the following possibilities apply:
  - If the AAA server protocol is RADIUS, then user roles specified in the cisco-av-pair attribute are downloaded with an authentication response.
  - If the AAA server protocol is TACACS+, then another request is sent to the same server to get the user roles specified as custom attributes for the shell.

- If your username and password are successfully authenticated locally, the Cisco Nexus 3000 Series switch logs you in and assigns you the roles configured in the local database.

Figure 1: Authorization and Authentication Flow for User Login



**Note**

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

## 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 3000 Series switch is configured as a client of the AAA servers.
- The preshared secret key is configured on the Cisco Nexus 3000 Series switch and on the remote AAA servers.
- The remote server responds to AAA requests from the Cisco Nexus 3000 Series switch.

## Information about AAA Guidelines and Limitations

The Cisco Nexus 3000 Series switches 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 login, the Cisco Nexus 3000 Series switch will still log in the user.

**Caution**

---

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

---

## Configuring AAA

### Configuring Console Login Authentication Methods

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

The authentication methods include the following:

- Global pool of RADIUS servers
- Named subset of RADIUS or TACACS+ servers
- Local database on the Cisco Nexus 3000 Series switch
- 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. To configure console login authentication methods, perform this task:

## SUMMARY STEPS

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

## DETAILED STEPS

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

The following 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 authentication methods include the following:

- Global pool of RADIUS servers

- Named subset of RADIUS or TACACS+ servers
- Local database on the Cisco Nexus 3000 Series switch
- Username only

The default method is local.

Before you configure default login authentication methods, configure RADIUS or TACACS+ server groups as needed. To configure default login authentication methods, perform this task:

## SUMMARY STEPS

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

## DETAILED STEPS

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

To enable login authentication failure messages, perform this task:

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>aaa authentication login error-enable</b>	Enables login authentication failure messages. The default is disabled.
<b>Step 3</b>	switch(config)# <b>exit</b>	Exits configuration mode.
<b>Step 4</b>	switch# <b>show aaa authentication</b>	(Optional) Displays the login failure message configuration.
<b>Step 5</b>	switch# <b>copy running-config startup-config</b>	(Optional) 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** There is no authorization on the console session.

### Before You Begin

You must enable TACACS+ before configuring AAA command authorization.

## SUMMARY STEPS

1. **configure terminal**
2. **aaa authorization {commands | config-commands} {default} {[group group-name] | [local]} | [group group-name] | [none]}**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>aaa authorization {commands   config-commands} {default} {[group group-name]   [local]}   [group group-name]   [none]}</b>  <b>Example:</b> <pre>switch(config)# aaa authorization config-commands default group tac1</pre> <b>Example:</b> <pre>switch# aaa authorization commands default group tac1</pre>	Configures authorization parameters.  Use the <b>commands</b> keyword to authorize EXEC mode commandes.  Use the <b>config-commands</b> keyword to authorize configuration mode commands.  Use the <b>group</b> , <b>local</b> , or <b>none</b> keywords to identify the authorization method.

The following shows EXEC and configuration mode examples.

This example shows how to authorize EXEC mode commands with TACACS+ server group *tac1*

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

This example shows how to authorize configuration mode commands with TACACS+ server group *tac1*

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

This 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
```

This 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
```

This example shows how to authorize EXEC mode commands regardless of the local role

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

This example shows how to authorize EXEC mode commands using the local role for authorization.

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

**Table 4: Related Commands**

Command	Descriptions
aaa server group	Configures AAA server groups.
feature tacacs+	Enables TACACS+.
tacacs-server host	Configures a TACACS+ server.

## 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 3000 Series switch through a remote authentication server (RADIUS or TACACS+).

By default, the Cisco Nexus 3000 Series switch uses Password Authentication Protocol (PAP) authentication between the switch and the remote server. If you enable MSCHAP, you need to configure your RADIUS server to recognize the MSCHAP vendor-specific attributes (VSAs).

The following table describes the RADIUS VSAs required for MSCHAP.

**Table 5: MSCHAP RADIUS VSAs**

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.

Vendor-ID Number	Vendor-Type Number	VSA	Description
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.

To enable MSCHAP authentication, perform this task:

## SUMMARY STEPS

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

## DETAILED STEPS

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

### Related Topics

[About VSAs, on page 20](#)

## Configuring AAA Accounting Default Methods

The Cisco Nexus 3000 Series switch 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 3000 Series switch 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 configure AAA accounting default methods, configure RADIUS or TACACS+ server groups as needed.

To configure AAA accounting default methods, perform this task:

**SUMMARY STEPS**

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

**DETAILED STEPS**

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

	Command or Action	Purpose
Step 4	switch# <b>show aaa accounting</b>	(Optional) Displays the configuration AAA accounting default methods.
Step 5	switch# <b>copy running-config startup-config</b>	(Optional) Copies the running configuration to the startup configuration.

## Using AAA Server VSAs

### About VSAs

You can use vendor-specific attributes (VSAs) to specify the Cisco Nexus 3000 Series 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 3000 Series switch, the RADIUS protocol directs the RADIUS server to return user attributes, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

### VSA Format

The following VSA protocol options are supported by the Cisco Nexus 3000 Series switches:

- 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 3000 Series switches:

- 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 3000 Series switch 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 *Cisco Nexus 3000 Series NX-OS System Management Configuration Guide*.

## Displaying and Clearing the Local AAA Accounting Log

The Cisco Nexus 3000 Series switch maintains a local log for the AAA accounting activity. To display this log and clear it, perform this task:

### SUMMARY STEPS

1. `switch# show accounting log [size] [start-time year month day hh : mm : ss]`
2. (Optional) `switch# clear accounting log`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>switch# show accounting log [size] [start-time year month day hh : mm : ss]</code>	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	<code>switch# clear accounting log</code>	(Optional) Clears the accounting log contents.

## Verifying AAA Configuration

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

### SUMMARY STEPS

1. `show aaa accounting`
2. `show aaa authentication [login {error-enable | mschap}]`
3. `show aaa authorization`
4. `show aaa groups`
5. `show running-config aaa [all]`
6. `show startup-config aaa`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>show aaa accounting</code>	Displays AAA accounting configuration.
Step 2	<code>show aaa authentication [login {error-enable   mschap}]</code>	Displays AAA authentication information.
Step 3	<code>show aaa authorization</code>	Displays AAA authorization information.
Step 4	<code>show aaa groups</code>	Displays the AAA server group configuration.
Step 5	<code>show running-config aaa [all]</code>	Displays the AAA configuration in the running configuration.
Step 6	<code>show startup-config aaa</code>	Displays the AAA configuration in the startup configuration.

## Example AAA Configuration

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 6: Default AAA Parameters**

<b>Parameters</b>	<b>Default</b>
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, page 25](#)

## 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 3000 Series switches 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 3000 Series switch with RADIUS to the network. This action might be the first step when you make a transition to a AAA server.

- Networks that require resource accounting.

You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider

(ISP) might use a freeware-based version of the RADIUS access control and accounting software to meet special security and billing needs.

- Networks that support authentication profiles.

Using the RADIUS server in your network, you can configure AAA authentication and set up per-user profiles. Per-user profiles enable the Nexus 5000 Series switch to better manage ports using their existing RADIUS solutions and to efficiently manage shared resources to offer different service-level agreements.

## RADIUS Operations

When a user attempts to log in and authenticate to a Cisco Nexus 3000 Series switch 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:

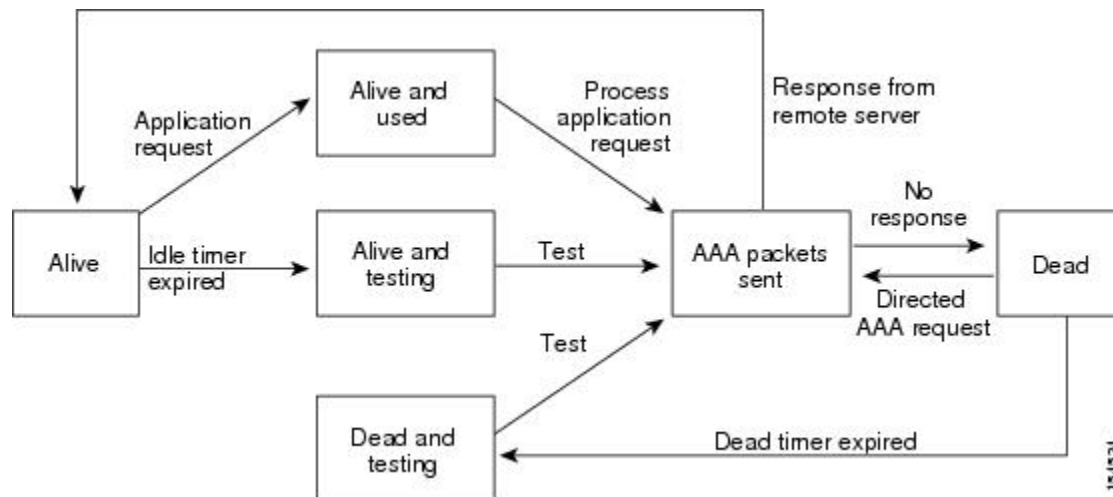
- Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IPv4 address, access list, and user timeouts.

## RADIUS Server Monitoring

An unresponsive RADIUS server can cause delay in processing of AAA requests. You can configure the Cisco Nexus 3000 Series switch to periodically monitor a RADIUS server to check whether it is responding (or alive) to save time in processing AAA requests. The Cisco Nexus 3000 Series 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 monitoring process verifies that a RADIUS server is in a working state before real AAA requests are sent its way. Whenever

a RADIUS server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Cisco Nexus 3000 Series switch displays an error message that a failure is taking place.

**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 3000 Series switch, the RADIUS protocol directs the RADIUS server to return user attributes, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

The following VSA protocol options are supported by the Cisco Nexus 3000 Series switch:

- 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.

Cisco Nexus 3000 Series switches support the following attributes:

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

- Obtain IPv4 addresses or host names for the RADIUS servers.
- Obtain preshared keys from the RADIUS servers.
- Ensure that the Cisco Nexus 3000 Series switch is configured as a RADIUS client of the AAA servers.

## Guidelines and Limitations for RADIUS

RADIUS has the following guidelines and limitations:

- You can configure a maximum of 64 RADIUS servers on the Cisco Nexus 3000 Series switch.

## Configuring RADIUS Servers

To configure RADIUS servers, perform this task:

### SUMMARY STEPS

1. Establish the RADIUS server connections to the Cisco Nexus 3000 Series switch.
2. Configure the preshared secret keys for the RADIUS servers.
3. If needed, configure RADIUS server groups with subsets of the RADIUS servers for AAA authentication methods.
4. If needed, configure any of the following optional parameters:
5. If needed, configure periodic RADIUS server monitoring.

### DETAILED STEPS

- 
- Step 1** Establish the RADIUS server connections to the Cisco Nexus 3000 Series switch.
- 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 host name 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.

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config) #	Enters global configuration mode.
<b>Step 2</b>	<b>radius-server host</b> <i>{ipv4-address   host-name}</i>  <b>Example:</b> switch(config) # radius-server host 10.10.1.1	Specifies the IPv4 address or hostname for a RADIUS server.
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> switch(config) # exit	Exits configuration mode.
<b>Step 4</b>	<b>show radius-server</b>  <b>Example:</b> switch# show radius-server	(Optional) Displays the RADIUS server configuration.

	Command or Action	Purpose
<b>Step 5</b>	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config) # copy running-config-startup-config switch(config) #</pre>	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

## Configuring RADIUS Global Preshared Keys

You can configure preshared keys at the global level for all servers used by the Cisco Nexus 3000 Series switch. 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

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config) #</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>radius-server key [0   7] key-value</b>  <b>Example:</b> <pre>switch(config)# radius-server key 0 QsEfThUkO</pre>	Specifies a preshared key for all RADIUS servers. You can specify a clear text ( <b>0</b> ) or encrypted ( <b>7</b> ) preshared key. The default format is clear text.  The maximum length is 63 characters.  By default, no preshared key is configured.
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit</pre>	Exits configuration mode.

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

## Configuring RADIUS Server Preshared Keys

A preshared key is a shared secret text string between the Cisco Nexus 3000 Series switch and the RADIUS server host.

### Before You Begin

Obtain the preshared key values for the remote RADIUS servers.

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config) #</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>radius-server host</b> { <i>ipv4-address</i>   <i>host-name</i> } <b>key</b> [0   7] <i>key-value</i>  <b>Example:</b> <pre>switch(config) # radius-server host 10.10.1.1 key 0 PlIjUhYg</pre>	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.

	Command or Action	Purpose
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> switch(config)# exit	Exits configuration mode.
<b>Step 4</b>	<b>show radius-server</b>  <b>Example:</b> switch# show radius-server	(Optional) Displays the RADIUS server configuration.  <b>Note</b> The preshared keys are saved in encrypted form in the running configuration. Use the <b>show running-config</b> command to display the encrypted preshared keys.
<b>Step 5</b>	<b>copy running-config startup-config</b>  <b>Example:</b> switch(config) # copy running-config-startup-config switch(config) #	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

## Configuring RADIUS Server Groups

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

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

### SUMMARY STEPS

1. **configure terminal**
2. **aaa group server radius** *group-name*
3. **server** {*ipv4-address* | *server-name*}
4. (Optional) **deadtime** *minutes*
5. (Optional) switch(config-radius)# **source-interface** *interface*
6. **exit**
7. (Optional) **show radius-server group** [*group-name*]
8. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config) #	Enters global configuration mode.
Step 2	<b>aaa group server radius <i>group-name</i></b>  <b>Example:</b> switch(config)# aaa group server radius RadServer	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 length of 127 characters.
Step 3	<b>server {<i>ipv4-address</i>   <i>server-name</i>}</b>  <b>Example:</b> switch(config-radius) # 10.10.1.1	Configures the RADIUS server as a member of the RADIUS server group.  If the specified RADIUS server is not found, configure it using the <b>radius-server host</b> command and retry this command.
Step 4	<b>deadtime <i>minutes</i></b>  <b>Example:</b> switch(config-radius) # deadtime 30	(Optional) Configures the monitoring dead time. The default is 0 minutes. The range is from 1 through 1440.  <b>Note</b> 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. See the example that shows how to configure periodic RADIUS server monitoring.
Step 5	switch(config-radius)# <b>source-interface <i>interface</i></b>  <b>Example:</b> switch(config-radius) # source-interface mgmt 0	(Optional) Assigns a source interface for a specific RADIUS server group.  The supported interface types are management and VLAN.  <b>Note</b> Use the <b>source-interface</b> command to override the global source interface assigned by the <b>ip radius source-interface</b> command.
Step 6	<b>exit</b>  <b>Example:</b> switch(config-radius) # exit	Exits configuration mode.
Step 7	<b>show radius-server group [<i>group-name</i>]</b>  <b>Example:</b> switch(config) # show radius-server group	(Optional) Displays the RADIUS server group configuration.
Step 8	<b>copy running-config startup-config</b>  <b>Example:</b> switch(config) # copy running-config-startup-config switch(config) #	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

**What to Do Next**

Apply them 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. Refer to the Related Commands for additional information.

**SUMMARY STEPS**

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

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config)	Enters global configuration mode.
<b>Step 2</b>	<b>ip radius source-interface <i>interface</i></b>  <b>Example:</b> switch(config)# ip radius source-interface mgmt 0	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.
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> switch(config)# exit switch#	Exits configuration mode.
<b>Step 4</b>	<b>show radius-server</b>  <b>Example:</b> switch# show radius-server	(Optional) Displays the RADIUS server configuration information.
<b>Step 5</b>	<b>copy running-config startup config</b>  <b>Example:</b> switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

**Related Commands**

Command	Description
<b>aaa group server radius group-name</b>	Creates a RADIUS server group and enters the RADIUS server group configuration submode for that group. The group-name argument is a case-sensitive alphanumeric string with a maximum length of 127 characters.

## Allowing Users to Specify a RADIUS Server at Login

To allow users to specify a RADIUS server at login, perform this task:

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server directed-request**
3. switch(config)# **exit**
4. (Optional) switch# **show radius-server directed-request**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

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

## 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 3000 Series switch waits for responses from RADIUS servers before declaring a timeout failure.

To configure the global RADIUS transmission retry count and timeout interval, perform this task:

## SUMMARY STEPS

1. **switch# configure terminal**
2. **switch(config)# radius-server retransmit *count***
3. **switch(config)# radius-server timeout *seconds***
4. **switch(config)# exit**
5. (Optional) **switch# show radius-server**
6. (Optional) **switch# copy running-config startup-config**

## DETAILED STEPS

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

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

By default, a Cisco Nexus 3000 Series 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.

## SUMMARY STEPS

1. **configure terminal**
2. **radius-server host {*ipv4-address* | *host-name*} retransmit *count***
3. **radius-server host {*ipv4-address* | *host-name*} timeout *seconds***
4. **exit**
5. (Optional) **switch# show radius-server**
6. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config) #</pre>	Enters global configuration mode.
Step 2	<b>radius-server host</b> { <i>ipv4-address</i>   <i>host-name</i> } <b>retransmit</b> <i>count</i>  <b>Example:</b> <pre>#switch(config)# radius-server host server1 retransmit 3</pre>	Specifies the retransmission count for a specific server. The default is the global value.  <b>Note</b> The retransmission count value specified for a RADIUS server overrides the count specified for all RADIUS servers.
Step 3	<b>radius-server host</b> { <i>ipv4-address</i>   <i>host-name</i> } <b>timeout</b> <i>seconds</i>  <b>Example:</b> <pre>switch(config) # radius-server host server1 timeout 10</pre>	Specifies the transmission timeout interval for a specific server. The default is the global value.  <b>Note</b> The timeout interval value specified for a RADIUS server overrides the interval value specified for all RADIUS servers.
Step 4	<b>exit</b>  <b>Example:</b> <pre>switch(config) # exit</pre>	Exits configuration mode.
Step 5	<b>switch# show radius-server</b>  <b>Example:</b> <pre>switch# show radius-server</pre>	(Optional) Displays the RADIUS server configuration.
Step 6	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config) # copy running-config-startup-config switch(config) #</pre>	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

## 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.

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config) #	Enters global configuration mode.
<b>Step 2</b>	<b>radius-server host</b> { <i>ipv4-address</i>   <i>host-name</i> } <b>acct-port</b> <i>udp-port</i>  <b>Example:</b> switch(config)# radius-server host 10.10.1.1 acct-port 2004	(Optional) Specifies a UDP port to use for RADIUS accounting messages. The default UDP port is 1812.  The range is from 0 to 65535.
<b>Step 3</b>	<b>radius-server host</b> { <i>ipv4-address</i>   <i>host-name</i> } <b>accounting</b>  <b>Example:</b> switch(config)# radius-server host 10.10.1.1 accounting	(Optional) Specifies that the specified RADIUS server it to be used only for accounting purposes. The default is both accounting and authentication.
<b>Step 4</b>	<b>radius-server host</b> { <i>ipv4-address</i>   <i>host-name</i> } <b>auth-port</b> <i>udp-port</i>  <b>Example:</b> switch(config)# radius-server host 10.10.2.2 auth-port 2005	(Optional) Specifies a UDP port to use for RADIUS authentication messages. The default UDP port is 1812.  The range is from 0 to 65535.
<b>Step 5</b>	<b>radius-server host</b> { <i>ipv4-address</i>   <i>host-name</i> } <b>authentication</b>  <b>Example:</b> switch(config)# radius-server host 10.10.2.2 authentication	(Optional) Specifies that the specified RADIUS server only be used for authentication purposes. The default is both accounting and authentication.

	Command or Action	Purpose
Step 6	<b>exit</b>  <b>Example:</b> switch(config)# <b>exit</b>	Exits configuration mode.
Step 7	<b>show radius-server</b>  <b>Example:</b> switch# <b>show radius-server</b>	(Optional) Displays the RADIUS server configuration.
Step 8	<b>copy running-config startup-config</b>  <b>Example:</b> switch(config) # copy running-config-startup-config switch(config) #	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

## 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.

### SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config) #</pre>	Enters global configuration mode.
Step 2	<b>radius-server host</b> { <i>ipv4-address</i>   <i>host-name</i> } <b>test</b> { <b>idle-time</b> <i>minutes</i>   <b>password</b> <i>password</i> [ <b>idle-time</b> <i>minutes</i> ]   <b>username</b> <i>name</i> [ <b>password</b> <i>password</i> [ <b>idle-time</b> <i>minutes</i> ]]}  <b>Example:</b> <pre>switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3</pre>	<p>Specifies parameters for server monitoring. The default username is test and the default password is test.</p> <p>The default value for the idle timer is 0 minutes.</p> <p>The valid range is 0 to 1440 minutes.</p> <p><b>Note</b> For periodic RADIUS server monitoring, you must set the idle timer to a value greater than 0.</p>
Step 3	<b>radius-server</b> <b>deadtime</b> <i>minutes</i>  <b>Example:</b> <pre>switch(config)# radius-server deadtime 5</pre>	<p>Specifies the number of minutes before the switch checks a RADIUS server that was previously unresponsive.</p> <p>The default value is 0 minutes.</p> <p>The valid range is 1 to 1440 minutes.</p>
Step 4	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit</pre>	Exits configuration mode.
Step 5	<b>show radius-server</b>  <b>Example:</b> <pre>switch# show radius-server</pre>	(Optional) Displays the RADIUS server configuration.
Step 6	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config) # copy running-config-startup-config switch(config) #</pre>	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

## 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 3000 Series switch 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.

To configure dead time interval, perform this task:

**SUMMARY STEPS**

1. switch# **configure terminal**
2. #switch(config)# **radius-server deadtime**
3. switch(config)# **exit**
4. (Optional) switch# **show radius-server**
5. (Optional) switch# **copy running-config startup-config**

**DETAILED STEPS**

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

**Manually Monitoring RADIUS Servers or Groups****SUMMARY STEPS**

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

## DETAILED STEPS

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

## Verifying RADIUS Configuration

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

## SUMMARY STEPS

1. **show running-config radius** [**all**]
2. **show startup-config radius**
3. **show radius-server** [*server-name* | *ipv4-address*] [**directed-request** | **groups** | **sorted** | **statistics**]

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>show running-config radius</b> [ <b>all</b> ]  <b>Example:</b> switch# <b>show running-config radius</b>	Displays the RADIUS configuration in the running configuration.
<b>Step 2</b>	<b>show startup-config radius</b>  <b>Example:</b> switch# <b>show startup-config radius</b>	Displays the RADIUS configuration in the startup configuration.
<b>Step 3</b>	<b>show radius-server</b> [ <i>server-name</i>   <i>ipv4-address</i> ] [ <b>directed-request</b>   <b>groups</b>   <b>sorted</b>   <b>statistics</b> ]  <b>Example:</b> switch# <b>show radius-server</b> radServer1	Displays all configured RADIUS server parameters.

## Displaying RADIUS Server Statistics

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>show radius-server statistics {hostname   ipv4-address}</code>  <b>Example:</b> <code>switch# show radius-server statistics 10.10.1.1</code>	Displays the RADIUS statistics.

## Example RADIUS Configuration

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 "ShMoMhTl" authentication accounting
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
switch(config-radius)# exit
switch(config-radius)# use-vrf management
```

## Default RADIUS Settings

The following table lists the default settings for RADIUS parameters.

**Table 7: 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

Parameters	Default
Periodic server monitoring password	test



## CHAPTER 5

# Configuring TACACS+

---

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

- [About Configuring TACACS+, page 45](#)

## About Configuring TACACS+

### Information About 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 3000 Series switch. 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 3000 Series switch 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. Cisco Nexus 3000 Series switches provide centralized authentication using the TACACS+ protocol.

### TACACS+ Advantages

TACACS+ has the following advantages over RADIUS authentication:

- Provides independent AAA facilities. For example, the Cisco Nexus 3000 Series switch 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 3000 Series switch using TACACS+, the following actions occur:

- 1 When the Cisco Nexus 3000 Series switch 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 3000 Series switch will receive one of the following responses from the TACACS+ daemon:
  - ACCEPT—User authentication succeeds and service begins. If the Cisco Nexus 3000 Series switch 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 3000 Series switch. If the Cisco Nexus 3000 Series switch 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 3000 Series switch. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

- 3 If TACACS+ authorization is required, the Cisco Nexus 3000 Series switch 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+ preshared key to authenticate the switch to the TACACS+ server. A preshared key is a secret text string shared between the Cisco Nexus 3000 Series switch 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 3000 Series switch to use.

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

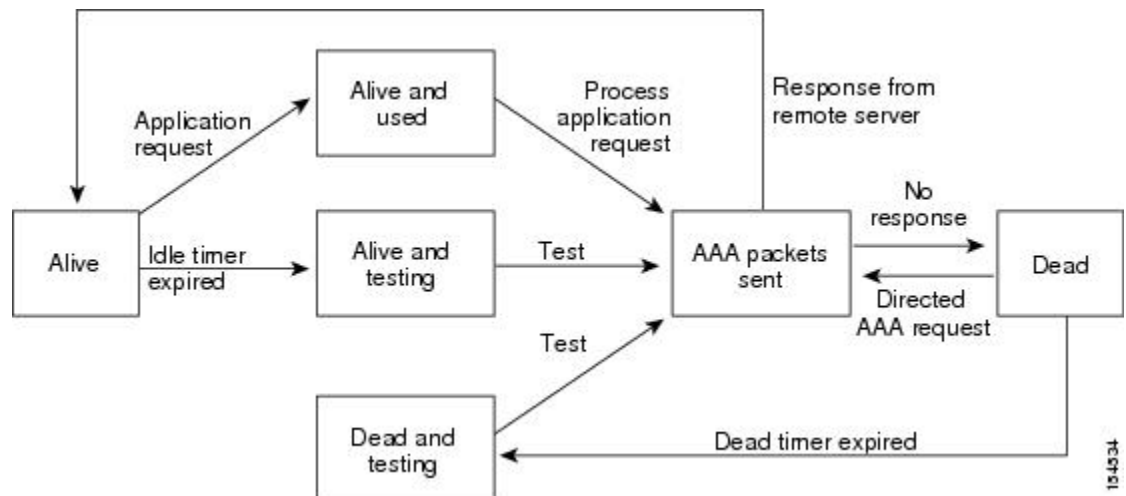
## Command Authorization Support for TACACS+ Servers

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

## TACACS+ Server Monitoring

An unresponsive TACACS+ server can delay the processing of AAA requests. A Cisco Nexus 3000 Series switch can periodically monitor an TACACS+ server to check whether it is responding (or alive) to save time in processing AAA requests. The Cisco Nexus 3000 Series switch marks unresponsive TACACS+ servers as dead and does not send AAA requests to any dead TACACS+ servers. A Cisco Nexus 3000 Series switch periodically monitors dead TACACS+ servers and brings them to the alive state once they are responding. This process verifies that a TACACS+ server is in a working state before real AAA requests are sent its way. Whenever an TACACS+ server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Cisco Nexus 3000 Series switch displays an error message that a failure is taking place before it can impact performance.

**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:

- Obtain the IPv4 addresses or host names for the TACACS+ servers.

- Obtain the preshared keys from the TACACS+ servers, if any.
- Ensure that the Cisco Nexus 3000 Series switch is configured as a TACACS+ client of the AAA servers.

## Guidelines and Limitations for TACACS+

TACACS+ has the following guidelines and limitations:

- You can configure a maximum of 64 TACACS+ servers on the Cisco Nexus 3000 Series switch.

## Configuring TACACS+

### TACACS+ Server Configuration Process

To configure TACACS+ servers, perform this task:

#### SUMMARY STEPS

1. Enable TACACS+.
2. Establish the TACACS+ server connections to the Cisco Nexus 3000 Series switch.
3. Configure the preshared secret keys for the TACACS+ servers.
4. If needed, configure TACACS+ server groups with subsets of the TACACS+ servers for AAA authentication methods.
5. If needed, configure any of the following optional parameters:
6. If needed, configure periodic TACACS+ server monitoring.

#### DETAILED STEPS

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Enable TACACS+.  |
| <b>Step 2</b> | Establish the TACACS+ server connections to the Cisco Nexus 3000 Series switch.  |
| <b>Step 3</b> | Configure the preshared secret keys for the TACACS+ servers.   |
| <b>Step 4</b> | If needed, configure TACACS+ server groups with subsets of the TACACS+ servers for AAA authentication methods.   |
| <b>Step 5</b> | If needed, configure any of the following optional parameters: <ul style="list-style-type: none"> <li>• Dead-time interval</li> <li>• Allow TACACS+ server specification at login</li> <li>• Timeout interval</li> <li>• TCP port</li> </ul> |
| <b>Step 6</b> | If needed, configure periodic TACACS+ server monitoring.   |
-

## Enabling TACACS+

By default, the TACACS+ feature is disabled on the Cisco Nexus 3000 Series switch. To explicitly enable the TACACS+ feature to access the configuration and verification commands for authentication, perform this task:

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>feature tacacs+</b>	Enables TACACS+.
<b>Step 3</b>	switch(config)# <b>exit</b>	Exits configuration mode.
<b>Step 4</b>	switch# <b>copy running-config startup-config</b>	(Optional) 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 3000 Series switch. 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.

To configure TACACS+ server hosts, perform this task:

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*}
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

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

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 3000 Series switch. A preshared key is a shared secret text string between the Cisco Nexus 3000 Series switch 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.

To configure global preshared keys, perform this task:

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>tacacs-server key [0   7] key-value</b>	Specifies a preshared key for all TACACS+ servers. You can specify a clear text ( <b>0</b> ) or encrypted ( <b>7</b> ) preshared key. The default format is clear text. The maximum length is 63 characters.  By default, no preshared key is configured.
<b>Step 3</b>	switch(config)# <b>exit</b>	Exits configuration mode.
<b>Step 4</b>	switch# <b>show tacacs-server</b>	(Optional) Displays the TACACS+ server configuration.  <b>Note</b> The preshared keys are saved in encrypted form in the running configuration. Use the <b>show running-config</b> command to display the encrypted preshared keys.
<b>Step 5</b>	switch# <b>copy running-config startup-config</b>	(Optional) Copies the running configuration to the startup configuration.

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
```

### Related Topics

[Enabling TACACS+ , on page 49](#)

## 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 3000 Series switch and the TACACS+ server host.

To configure the TACACS+ preshared keys, perform this task:

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>tacacs-server host</b> { <i>ipv4-address</i>   <i>host-name</i> } <b>key</b> [0   7] <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.
<b>Step 3</b>	switch(config)# <b>exit</b>	Exits configuration mode.
<b>Step 4</b>	switch# <b>show tacacs-server</b>	(Optional) Displays the TACACS+ server configuration.  <b>Note</b> The preshared keys are saved in encrypted form in the running configuration. Use the <b>show running-config</b> command to display the encrypted preshared keys.
<b>Step 5</b>	switch# <b>copy running-config startup-config</b>	(Optional) Copies the running configuration to the startup configuration.

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 P1IjUhYg
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+.

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **aaa group server tacacs+ group-name**
3. switch(config)# **tacacs-server host {ipv4-address | host-name} key [0 | 7] key-value**
4. (Optional) switch(config-tacacs+)# **deadtime minutes**
5. (Optional) switch(config-tacacs+)# **source-interface interface**
6. switch(config-tacacs+)# **exit**
7. (Optional) switch(config)# **show tacacs-server groups**
8. (Optional) switch(config)# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>aaa group server tacacs+ group-name</b>	Creates a TACACS+ server group and enters the TACACS+ server group configuration mode for that group.
<b>Step 3</b>	switch(config)# <b>tacacs-server host {ipv4-address   host-name} key [0   7] key-value</b>	Specifies a preshared key for a specific TACACS+ server. You can specify a clear text ( <b>0</b> ) or encrypted ( <b>7</b> ) 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.
<b>Step 4</b>	switch(config-tacacs+)# <b>deadtime minutes</b>  <b>Example:</b>	(Optional) Configures the monitoring dead time. The default is 0 minutes. The range is from 0 through 1440.  <b>Note</b> 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.
<b>Step 5</b>	switch(config-tacacs+)# <b>source-interface interface</b>  <b>Example:</b> switch(config-tacacs+)# <b>source-interface mgmt 0</b>	(Optional) Assigns a source interface for a specific TACACS+ server group.  The supported interface types are management and VLAN.  <b>Note</b> Use the <b>source-interface</b> command to override the global source interface assigned by the <b>ip tacacs source-interface</b> command.
<b>Step 6</b>	switch(config-tacacs+)# <b>exit</b>	Exits configuration mode.
<b>Step 7</b>	switch(config)# <b>show tacacs-server groups</b>	(Optional) Displays the TACACS+ server group configuration.
<b>Step 8</b>	switch(config)# <b>copy running-config startup-config</b>	(Optional) Copies the running configuration to the startup configuration.

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
```

**Table 8: Related Commands**

Command	Description
<b>feature tacacs+</b>	Enables the TACACS+ feature.
<b>ip tacacs source-interface</b>	Configures the global source interface for the TACACS+ groups configured on the Cisco NX-OS device.
<b>show tacacs-server groups</b>	Displays the TACACS+ server group configuration.

### 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. Refer to Related Commands for additional information.

#### SUMMARY STEPS

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

#### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config)	Enters global configuration mode.
<b>Step 2</b>	<b>ip tacacs source-interface</b> <i>interface</i>  <b>Example:</b> 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.

	Command or Action	Purpose
Step 3	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	<b>show tacacs-server</b>  <b>Example:</b> <pre>switch# show tacacs-server</pre>	(Optional) Displays the TACACS+ server configuration information.
Step 5	<b>copy running-config startup config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

Table 9: Related Commands

Command	Description
<b>aaa group server tacacs group-name</b>	Creates a TACACS+ server group and enters the TACACS+ server group configuration submode for that group. The group-name argument is a case-sensitive alphanumeric string with a maximum length of 127 characters.

### 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 3000 Series switch 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.

To specify a TACACS+ server at login, perform this task:

### SUMMARY STEPS

1. `switch# configure terminal`
2. `switch(config)# tacacs-server directed-request`
3. `switch(config)# exit`
4. (Optional) `switch# show tacacs-server directed-request`
5. (Optional) `switch# copy running-config startup-config`

## DETAILED STEPS

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

## Configuring AAA Authorization on TACACS+ Servers

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

**Before You Begin**

Enable TACACS+.

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> switch# <code>configure terminal</code> switch(config)#	Enters global configuration mode.
Step 2	<b>aaa authorization ssh-certificate default {group group-list [none]   local   none}</b>	Configures the default AAA authorization method for the TACACS+ servers.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>switch(config)# aaa authorization ssh-certificate default group TACACSServer1 TACACSServer2</pre>	<p>The <b>ssh-certificate</b> 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 <b>local</b> method uses the local database for authorization, and the <b>none</b> method specifies that no AAA authorization be used.</p>
<b>Step 3</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
<b>Step 4</b>	<p><b>show aaa authorization [all]</b></p> <p><b>Example:</b></p> <pre>switch# show aaa authorization</pre>	(Optional) Displays the AAA authorization configuration. The <b>all</b> keyword displays the default values.
<b>Step 5</b>	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

### 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.



**Note** By default, context sensitive help and command tab completion show only the commands that are supported for a user as defined by the assigned roles. When you enable command authorization, the Cisco NX-OS software displays all commands in the context sensitive help and in tab completion, regardless of the role assigned to the user.

#### Before You Begin

Enable TACACS+.

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

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>aaa authorization {commands   config-commands} default [group group-list [local]   local]</b>  <b>Example:</b> <pre>switch(config)# aaa authorization commands default group TacGroup</pre>	<p>Configures the default authorization method for commands for all roles. The <b>commands</b> keyword configures authorization sources for all EXEC commands, and the <b>config-commands</b> 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 <b>local</b> method uses the local role-based database for authorization..</p> <p>The <b>local</b> method is used only if all the configured server groups fail to respond and you have configured <b>local</b> as the fallback method.</p> <p>The default method is <b>local</b>.</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>
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
<b>Step 4</b>	<b>show aaa authorization [all]</b>  <b>Example:</b> <pre>switch(config)# show aaa authorization</pre>	(Optional) Displays the AAA authorization configuration. The <b>all</b> keyword displays the default values.
<b>Step 5</b>	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	(Optional) 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.

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>test aaa authorization command-type {commands   config-commands} user username command command-string</b>  <b>Example:</b> <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 <b>commands</b> keyword specifies only EXEC commands and the <b>config-commands</b> keyword specifies only configuration commands.  <b>Note</b> 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.

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>terminal verify-only</b> [username <i>username</i> ]  <b>Example:</b> 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.
<b>Step 2</b>	<b>terminal no verify-only</b> [username <i>username</i> ]  <b>Example:</b> 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"> <li>Standalone role permissions, if the <b>feature privilege</b> command is disabled.</li> <li>Same permissions as privilege level 0 with cumulative privileges for roles, if the <b>feature privilege</b> command is enabled.</li> </ul>
0	Permission to execute <b>show</b> commands and <b>exec</b> commands (such as <b>ping</b> , <b>trace</b> , and <b>ssh</b> ).



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

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] feature privilege</b>  <b>Example:</b> <pre>switch(config)# feature privilege</pre>	Enables or disables the cumulative privilege of roles. Users can see the <b>enable</b> command only if this feature is enabled. The default is disabled.
<b>Step 3</b>	<b>[no] enable secret [0   5] password [priv-lvl priv-lvl   all]</b>  <b>Example:</b> <pre>switch(config)# enable secret 5 def456 priv-lvl 15</pre>	<p>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.</p> <p>You can enter <b>0</b> to specify that the password is in clear text or <b>5</b> 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.</p> <p><b>Note</b> To enable the secret password, you must have enabled the cumulative privilege of roles by entering the <b>feature privilege</b> command.</p>
<b>Step 4</b>	<b>[no] username username priv-lvl n</b>  <b>Example:</b> <pre>switch(config)# username user2 priv-lvl 15</pre>	<p>Enables or disables a user to use privilege levels for authorization. The default is disabled.</p> <p>The <b>priv-lvl</b> 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.</p>
<b>Step 5</b>	<b>show privilege</b>  <b>Example:</b> <pre>switch(config)# show privilege</pre>	<p>(Optional)</p> <p>Displays the username, current privilege level, and status of cumulative privilege support.</p>

	Command or Action	Purpose
<b>Step 6</b>	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.
<b>Step 7</b>	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
<b>Step 8</b>	<b>enable level</b>  <b>Example:</b> <pre>switch# enable 15</pre>	Enables a user to move to a higher privilege level. This command prompts for the secret password. The <i>level</i> argument specifies the 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**.

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	<p><b>[no] role name priv-<i>n</i></b></p> <p><b>Example:</b>  <pre>switch(config)# role name priv-5 switch(config-role)#</pre></p>	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	<p><b>rule number {deny   permit} command</b>  <i>command-string</i></p> <p><b>Example:</b>  <pre>switch(config-role)# rule 2 permit command pwd</pre></p>	<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><b>Note</b> Repeat this command for 256 rules.</p>
Step 4	<p><b>exit</b></p> <p><b>Example:</b>  <pre>switch(config-role)# exit switch(config)#</pre></p>	Exits role configuration mode.
Step 5	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b>  <pre>switch(config)# copy running-config startup-config</pre></p>	(Optional) 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 3000 Series switch 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.

To specify a TACACS+ global timeout interval, perform this task:

#### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server timeout** *seconds*
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>tacacs-server timeout seconds</b>	Specifies the timeout interval for TACACS+ servers. The default timeout interval is 5 second and the range is from 1 to 60 seconds.
<b>Step 3</b>	switch(config)# <b>exit</b>	Exits configuration mode.
<b>Step 4</b>	switch# <b>show tacacs-server</b>	(Optional) Displays the TACACS+ server configuration.
<b>Step 5</b>	switch# <b>copy running-config startup-config</b>	(Optional) 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 3000 Series switch 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.

To configure the timeout interval for a server, perform this task:

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# switch(config)# **tacacs-server host {ipv4-address | host-name} timeout seconds**
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# switch(config)# <b>tacacs-server host {ipv4-address   host-name} timeout seconds</b>	Specifies the timeout interval for a specific server. The default is the global value.  <b>Note</b> The timeout interval value specified for a TACACS+ server overrides the global timeout interval value specified for all TACACS+ servers.
<b>Step 3</b>	switch(config)# <b>exit</b>	Exits configuration mode.

	Command or Action	Purpose
<b>Step 4</b>	switch# <b>show tacacs-server</b>	(Optional) Displays the TACACS+ server configuration.
<b>Step 5</b>	switch# <b>copy running-config startup-config</b>	(Optional) 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, Cisco Nexus 3000 Series switches use port 49 for all TACACS+ requests.

To configure TCP ports, perform this task:

#### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **port** *tcp-port*
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

#### DETAILED STEPS

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

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 3000 Series switch 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 user name 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 3000 Series switch 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.

To configure periodic TACACS+ server monitoring, perform this task:

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>tacacs-server host</b> { <i>ipv4-address</i>   <i>host-name</i> } <b>test</b> { <i>idle-time minutes</i>   <b>password</b> <i>password</i> [ <i>idle-time minutes</i> ]   <b>username</b> <i>name</i> [ <b>password</b> <i>password</i> [ <i>idle-time 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 0 to 1440 minutes. <b>Note</b> For periodic TACACS+ server monitoring, the idle timer value must be greater than 0.
<b>Step 3</b>	switch(config)# <b>tacacs-server dead-time</b> <i>minutes</i>	Specifies the number minutes before the Cisco Nexus 3000 Series switch checks a TACACS+ server that was previously unresponsive. The default value is 0 minutes and the valid range is 0 to 1440 minutes.

	Command or Action	Purpose
Step 4	switch(config)# <b>exit</b>	Exits configuration mode.
Step 5	switch# <b>show tacacs-server</b>	(Optional) Displays the TACACS+ server configuration.
Step 6	switch# <b>copy running-config startup-config</b>	(Optional) Copies the running configuration to the startup configuration.

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 3000 Series switch waits, after declaring a TACACS+ server is dead, before sending out a test packet to determine if the server is now alive.



#### Note

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

To configure the dead-time interval for all TACACS+ servers, perform this task:

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server deadtime** *minutes*
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# <b>configure terminal</b>	Enters configuration mode.
Step 2	switch(config)# <b>tacacs-server deadtime</b> <i>minutes</i>	Configures the global dead-time interval. The default value is 0 minutes. The range is from 1 to 1440 minutes.

	Command or Action	Purpose
<b>Step 3</b>	switch(config)# <b>exit</b>	Exits configuration mode.
<b>Step 4</b>	switch# <b>show tacacs-server</b>	(Optional) Displays the TACACS+ server configuration.
<b>Step 5</b>	switch# <b>copy running-config startup-config</b>	(Optional) Copies the running configuration to the startup configuration.

### Manually Monitoring TACACS+ Servers or Groups

To manually issue a test message to a TACACS+ server or to a server group, perform this task:

#### SUMMARY STEPS

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

#### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>test aaa server tacacs+</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>host-name</i> } [ <b>vrf</b> <i>vrf-name</i> ] <i>username password</i>	Sends a test message to a TACACS+ server to confirm availability.
<b>Step 2</b>	switch# <b>test aaa group</b> <i>group-name username password</i>	Sends a test message to a TACACS+ server group to confirm availability.

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.

To disable TACACS+, perform this task:

**SUMMARY STEPS**

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

**DETAILED STEPS**

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

**Displaying TACACS+ Statistics**

To display the statistics the Cisco Nexus 3000 Series switch maintains for TACACS+ activity, perform this task:

**SUMMARY STEPS**

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

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	switch# <b>show tacacs-server statistics</b> {hostname   ipv4-address   ipv6-address}	Displays the TACACS+ statistics.

For detailed information about the fields in the output from this command, see the *Cisco Nexus 3000 Series Command Reference*.

**Verifying TACACS+ Configuration**

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

## SUMMARY STEPS

1. switch# show tacacs+ {status | pending | pending-diff}
2. switch# show running-config tacacs [all]
3. switch# show startup-config tacacs
4. switch# show tacacs-serve [host-name | ipv4-address] [directed-request | groups | sorted | statistics]

## DETAILED STEPS

	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.
Step 4	switch# show tacacs-serve [host-name   ipv4-address] [directed-request   groups   sorted   statistics]	Displays all configured TACACS+ server parameters.

## Configuration Examples for TACACS+

The following 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
```

The following 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# config t
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 TACACS+ Settings

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

**Table 10: Default TACACS+ Parameters**

<b>Parameters</b>	<b>Default</b>
TACACS+	Disabled
Dead timer interval	0 minutes
Timeout interval	5 seconds
Idle timer interval	0 minutes
Periodic server monitoring username	test
Periodic server monitoring password	test





## CHAPTER 6

# Configuring SSH and Telnet

---

This chapter describes how to configure Secure Shell Protocol (SSH) and Telnet on Cisco NX-OS devices.

- [Configuring SSH and Telnet, page 73](#)

## 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 3000 Series switch. SSH uses strong encryption for authentication. The SSH server in the Cisco Nexus 3000 Series switch will interoperate 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 Cisco Nexus 3000 Series switch to make a secure, encrypted connection to another Cisco Nexus 3000 Series switch 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 3000 Series switch works with publicly and commercially available SSH servers.

#### SSH Server Keys

SSH requires server keys for secure communications to the Cisco Nexus 3000 Series switch. 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 3000 Series switch 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 3000 Series switch.

## Guidelines and Limitations for SSH

SSH has the following configuration guidelines and limitations:

- The Cisco Nexus 3000 Series switch 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 generated using 1024 bits. To generate SSH server keys, perform this task:

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **ssh key {dsa [force] | rsa [bits [force]]}**
3. switch(config)# **exit**
4. (Optional) switch# **show ssh key**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>ssh key {dsa [force]   rsa [bits [force]]}</b>	Generates the SSH server key. The <i>bits</i> argument is the number of bits used to generate the key. The range is 768 to 2048 and the default value is 1024. Use the <b>force</b> keyword to replace an existing key.
<b>Step 3</b>	switch(config)# <b>exit</b>	Exits global configuration mode.
<b>Step 4</b>	switch# <b>show ssh key</b>	(Optional) Displays the SSH server keys.
<b>Step 5</b>	switch# <b>copy running-config startup-config</b>	(Optional) Copies the running configuration to the startup configuration.

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.

To specify the SSH public keys in open SSH format, generate an SSH public key in open SSH format and perform this task:

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **username** *username* **sshkey** *ssh-key*
3. switch(config)# **exit**
4. (Optional) switch# **show user-account**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

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

The following example shows how to specify an SSH public keys 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 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.

To specify the SSH public keys in IETF SECSH format, generate an SSH public key in IETF SCHSH format, and perform this task:

## SUMMARY STEPS

1. switch# **copy server-file bootflash: filename**
2. switch# **configure terminal**
3. switch(config)# **username username sshkey file filename**
4. switch(config)# **exit**
5. (Optional) switch# **show user-account**
6. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

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

The following example shows how to specify the SSH public keys 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.

To specify the SSH public keys in PEM-formatted Public Key Certificate form, generate an SSH public key in PEM-Formatted Public Key Certificate form and perform this task:

**SUMMARY STEPS**

1. switch# **copy server-file bootflash: filename**
2. switch# **configure terminal**
3. (Optional) switch# **show user-account**
4. (Optional) switch# **copy running-config startup-config**

**DETAILED STEPS**

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

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**

To start SSH sessions to connect to remote devices from your Cisco Nexus 3000 Series switch, perform this task:

**SUMMARY STEPS**

1. switch# **ssh {hostname | username@hostname} [vrf vrf-name]**

**DETAILED STEPS**

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

## Clearing SSH Hosts

When you download a file from a server using SCP or SFTP, you establish a trusted SSH relationship with that server. To clear the list of trusted SSH servers for your user account, perform this task:

### SUMMARY STEPS

1. switch# **clear ssh hosts**

### DETAILED STEPS

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

## Disabling the SSH Server

By default, the SSH server is enabled on the Cisco Nexus 3000 Series switch.

To disable the SSH server to prevent SSH access to the switch, perform this task:

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no feature ssh**
3. switch(config)# **exit**
4. (Optional) switch# **show ssh server**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# <b>configure terminal</b>	Enters configuration mode.
Step 2	switch(config)# <b>no feature ssh</b>	Disables the SSH server. The default is enabled.
Step 3	switch(config)# <b>exit</b>	Exits global configuration mode.
Step 4	switch# <b>show ssh server</b>	(Optional) Displays the SSH server configuration.
Step 5	switch# <b>copy running-config startup-config</b>	(Optional) 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 reenab SSH, you must first generate an SSH server key.

To delete the SSH server keys, perform this task:

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no feature ssh**
3. switch(config)# **no ssh key [dsa | rsa]**
4. switch(config)# **exit**
5. (Optional) switch# **show ssh key**
6. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

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

## Clearing SSH Sessions

To clear SSH sessions from the Cisco Nexus 3000 Series switch, perform this task:

### SUMMARY STEPS

1. switch# **show users**
2. switch# **clear line vty-line**

## DETAILED STEPS

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

## SSH Example Configuration

The following example shows how to configure SSH:

### SUMMARY STEPS

1. Generate an SSH server key.
2. Enable the SSH server.
3. Display the SSH server key.
4. Specify the SSH public key in Open SSH format.
5. Save the configuration.

### DETAILED STEPS

**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 as 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 AAAAB3NzaClyc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYzCfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZ/
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 AAAAB3NzaC1yc2EAAAABIwAAAEArI3mQy4W1AV9Y2t2hrEWgbUEYz
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dqBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rzZt0KR+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 3000 Series switch.

#### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature telnet**

#### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>feature telnet</b>	Disables the Telnet server. The default is enabled.

### Reenabling the Telnet Server

If the Telnet server on your Cisco Nexus 3000 Series switch has been disabled, you can reenabling it.

#### SUMMARY STEPS

1. switch(config)# **feature telnet**

**DETAILED STEPS**

	Command or Action	Purpose
Step 1	switch(config)# <b>feature telnet</b>	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, the user name on the remote device.
- Enable the Telnet server on the Cisco Nexus 3000 Series switch.
- Enable the Telnet server on the remote device.

To start Telnet sessions to connect to remote devices from your Cisco Nexus 3000 Series switch, perform this task:

**SUMMARY STEPS**

1. switch# **telnet** *hostname*

**DETAILED STEPS**

	Command or Action	Purpose
Step 1	switch# <b>telnet</b> <i>hostname</i>	Creates a Telnet session to a remote device. The <i>hostname</i> argument can be an IPv4 address, an IPv6 address, or a device name.

The following example shows starting 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**

To clear Telnet sessions from the Cisco Nexus 3000 Series switch, perform this task:

**SUMMARY STEPS**

1. switch# **show users**
2. switch# **clear line** *vtty-line*

## DETAILED STEPS

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

## Verifying the SSH and Telnet Configuration

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

- switch# **show ssh key [dsa | rsa]**  
Displays SSH server key-pair information.
- switch# **show running-config security [all]**  
Displays the SSH and user account configuration in the running configuration. The **all** keyword displays the default values for the SSH and user accounts.
- switch# **show ssh server**  
Displays the SSH server configuration.
- switch# **show user-account**  
Displays user account information.

## Default SSH Settings

The following table lists the default settings for SSH parameters.

**Table 11: 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, page 85](#)
- [Configuring IP ACLs, page 88](#)
- [Information About VLAN ACLs, page 95](#)
- [Configuring VACLs, page 96](#)
- [Configuration Examples for VACL, page 99](#)
- [Configuring ACL TCAM Region Sizes, page 99](#)
- [Configuring ACLs on Virtual Terminal Lines, page 102](#)
- [Default ACL Settings, page 104](#)

## 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 3000 Series switch supports IPv4 for security traffic filtering. The switch allows you to use IP access control lists (ACLs) as port ACLs and VLAN ACLs as shown in the following table.

**Table 12: 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"> <li>• Ethernet interface</li> <li>• Ethernet port-channel interface</li> </ul> <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
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

## Application Order

When the switch processes a packet, it determines the forwarding path of the packet. The path determines which ACLs that the switch applies to the traffic. The switch applies the Port ACLs first.

## Rules

You can create rules in access-list configuration mode by using the **permit** or **deny** command. The switch 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.

## 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

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 number. In IPv4 ACLs, you can specify protocols by the integer that represents the Internet protocol number.

## Implicit Rules

IP 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.

## 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 switch supports sequence numbers for rules. Every rule that you enter receives a sequence number, either assigned by you or assigned automatically by the switch. 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 switch 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 switch assigns the sequence number 235 to the new rule.

In addition, the Cisco Nexus 3000 Series switch 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 switch stores operator-operand couples in registers called logical operator units (LOUs).

LOU usage for the "eq" operator is never stored in an LOU. The range operation is inclusive of boundary values.

The following guidelines determine when the switch 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.

# Configuring IP ACLs

## Creating an IP ACL

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

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **ip access-list name**
3. switch(config)# **ip access-list name**
4. switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*
5. (Optional) switch(config-acl)# **statistics**
6. (Optional) switch# **show ip access-lists name**
7. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# <b>configure terminal</b>	Enters configuration mode.
Step 2	switch(config)# <b>ip access-list name</b>	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)# <b>ip access-list name</b>	Creates the IP ACL and enters IP ACL configuration mode. The <i>name</i> argument can be up to 64 characters.
Step 4	switch(config-acl)# [ <i>sequence-number</i> ] <b>{permit   deny} protocol source destination</b>	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 <b>permit</b> and <b>deny</b> commands support many ways of identifying traffic. For more information, see the <i>Cisco Nexus 3000 Series Command Reference</i> .
Step 5	switch(config-acl)# <b>statistics</b>	(Optional) Specifies that the switch maintains global statistics for packets that matches the rules in the ACL.
Step 6	switch# <b>show ip access-lists name</b>	(Optional) Displays the IP ACL configuration.
Step 7	switch# <b>copy running-config startup-config</b>	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to create an IPv4 ACL:

```
switch# configure terminal
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.

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)#**ip access-list name**
3. switch(config-acl)# [*sequence-number*] **{permit | deny}** *protocol source destination*
4. (Optional) switch(config-acl)# **no** {*sequence-number* | **{permit | deny}** *protocol source destination*}
5. (Optional) switch(config-acl)# [**no**] **statistics**
6. (Optional) switch#**show ip access-lists name**
7. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>ip access-list name</b>	Enters IP ACL configuration mode for the ACL that you specify by name.
<b>Step 3</b>	switch(config-acl)# [ <i>sequence-number</i> ] <b>{permit   deny}</b> <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 <b>permit</b> and <b>deny</b> commands support many ways of identifying traffic. For more information, see the <i>Cisco Nexus 3000 Series Command Reference</i> .
<b>Step 4</b>	switch(config-acl)# <b>no</b> { <i>sequence-number</i>   <b>{permit   deny}</b> <i>protocol source destination</i> }	(Optional) Removes the rule that you specified from the IP ACL.  The <b>permit</b> and <b>deny</b> commands support many ways of identifying traffic. For more information, see the <i>Cisco Nexus 3000 Series Command Reference</i> .
<b>Step 5</b>	switch(config-acl)# [ <b>no</b> ] <b>statistics</b>	(Optional) Specifies that the switch maintains global statistics for packets matching the rules in the ACL.  The <b>no</b> option stops the switch from maintaining global statistics for the ACL.
<b>Step 6</b>	switch# <b>show ip access-lists name</b>	(Optional) Displays the IP ACL configuration.
<b>Step 7</b>	switch# <b>copy running-config startup-config</b>	(Optional) Copies the running configuration to the startup configuration.

## Related Topics

[Changing Sequence Numbers in an IP ACL, on page 91](#)

## 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.

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no ip access-list name**
3. (Optional) switch# **show running-config**
4. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

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

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **resequence ip access-list name starting-sequence-number increment**
3. (Optional) switch# **show ip access-lists name**
4. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# <b>configure terminal</b>	Enters configuration mode.
Step 2	switch(config)# <b>resequence ip access-list</b> <i>name starting-sequence-number increment</i>	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	switch# <b>show ip access-lists</b> <i>name</i>	(Optional) Displays the IP ACL configuration.
Step 4	switch# <b>copy running-config</b> <b>startup-config</b>	(Optional) 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.

## SUMMARY STEPS

1. **configure terminal**
2. **interface mgmt** *port*
3. **ip access-group** *access-list* {in | out}
4. (Optional) **show running-config aclmgr**
5. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> switch(config)#	Enters global configuration mode.

	Command or Action	Purpose
Step 2	<b>interface</b> <i>mgmt port</i>  <b>Example:</b> <pre>switch(config)# interface mgmt0 switch(config-if)#</pre>	Enters configuration mode for the management interface.
Step 3	<b>ip access-group</b> <i>access-list {in   out}</i>  <b>Example:</b> <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	<b>show running-config aclmgr</b>  <b>Example:</b> <pre>switch(config-if)# show running-config aclmgr</pre>	(Optional) Displays the ACL configuration.
Step 5	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-if)# copy running-config startup-config</pre>	(Optional) 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 EtherChannel are not reflected on the configuration of the member ports.

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {*ethernet [chassis/]slot/port* | **port-channel** *channel-number*}
3. switch(config-if)# **ip port access-group** *access-list in*
4. switch(config-if)# **ip port access-group** *access-list in*
5. (Optional) switch# **show running-config**
6. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>interface</b> { <b>ethernet</b> [ <i>chassis/</i> ] <i>slot/port</i>   <b>port-channel</b> <i>channel-number</i> }	Enters interface configuration mode for the specified interface.
<b>Step 3</b>	switch(config-if)# <b>ip port access-group</b> <i>access-list</i> <b>in</b>	Applies an IPv4 ACL to the interface or EtherChannel. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.
<b>Step 4</b>	switch(config-if)# <b>ip port access-group</b> <i>access-list</i> <b>in</b>	Applies an IPv4 ACL to the interface or EtherChannel. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.
<b>Step 5</b>	switch# <b>show running-config</b>	(Optional) Displays the ACL configuration.
<b>Step 6</b>	switch# <b>copy running-config startup-config</b>	(Optional) Copies the running configuration to the startup configuration.

## Verifying IP ACL Configurations

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

- 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.

For detailed information about the fields in the output from these commands, refer to the *Cisco Nexus 3000 Series Command Reference*.

## 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 *Cisco Nexus 3000 Series Command Reference*.

**Note**

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

- 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.

## Information About VLAN ACLs

A VLAN ACL (VACL) is one application of a 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).

**Note**

---

If an IPv4 ACL, applied as a VLAN ACL, contains one or more ACEs with logical operators for TCP/UDP port numbers, the port numbers are matched in the ingress direction but ignored in the egress direction.

---

VACLs have the following restrictions:

- 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.

## VACLs and Access Maps

VACLs use access maps to link an IP ACL to an action. The switch takes the configured action on packets 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 switch 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 3000 Series switch 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.

To create or change a VACL, perform this task:

#### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan access-map** *map-name*
3. switch(config-access-map)# **match ip address** *ip-access-list*
4. switch(config-access-map)# **action** {**drop** | **forward**}
5. (Optional) switch(config-access-map)# [**no**] **statistics**
6. (Optional) switch(config-access-map)# **show running-config**
7. (Optional) switch(config-access-map)# **copy running-config startup-config**

#### DETAILED STEPS

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

	Command or Action	Purpose
Step 7	switch(config-access-map)# <b>copy running-config startup-config</b>	(Optional) 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.

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no vlan access-map** *map-name*
3. (Optional) switch(config)# **show running-config**
4. (Optional) switch(config)# **copy running-config startup-config**

### DETAILED STEPS

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

## Applying a VACL to a VLAN

You can apply a VACL to a VLAN.

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **[no] vlan filter map-name vlan-list list**
3. (Optional) switch(config)# **show running-config**
4. (Optional) switch(config)# **copy running-config startup-config**

**DETAILED STEPS**

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

**Verifying VACL Configuration**

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

- 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:

- 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.

### SUMMARY STEPS

1. **configure terminal**
2. **hardware profile tcam region {arpacl | e-racl | ifacl | ipsg | qos | qoslbl | racl | vacl } tcam\_size**
3. (Optional) **copy running-config startup-config**
4. **switch(config)# show hardware profile tcam region**
5. **switch(config)# reload**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config) #	Enters global configuration mode.
Step 2	<b>hardware profile tcam region {arpacl   e-racl   ifacl   ipsg   qos   qoslbl   racl   vacl } tcam_size</b>	Changes the ACL TCAM region size. <ul style="list-style-type: none"> <li>• <b>arpacl</b>—Configures the size of the Address Resolution Protocol (ARP) ACL (ARPAcl) TCAM region.</li> <li>• <b>e-racl</b>—Configures the size of the egress router ACL (ERACL) TCAM region.</li> <li>• <b>e-vacl</b>—Configures the size of the egress VLAN ACL (EVACL) TCAM region.</li> <li>• <b>ifacl</b>—Configures the size of the interface ACL (ifacl) TCAM region.</li> <li>• <b>ipsg</b>—Configures the size of the IP Source Guard (IPSG) TCAM region.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• <b>qos</b>—Configures the size of the quality of service (QoS) TCAM region.</li> <li>• <b>qoslbl</b>—Configures the size of the QoS Label (qoslbl) TCAM region.</li> <li>• <b>racl</b>—Configures the size of the router ACL (RACL) TCAM region.</li> <li>• <b>vacl</b>—Configures the size of the VLAN ACL (VACL) TCAM region.</li> <li>• <b>tcam_size</b>—TCAM size. The range is from 0 to 2,14,74, 83, 647 entries.</li> </ul>
<b>Step 3</b>	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config) # copy running-config-startup-config switch(config) #</pre>	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.
<b>Step 4</b>	switch(config)# <b>show hardware profile tcam region</b>	Displays the TCAM sizes that will be applicable on the next reload of the switch.
<b>Step 5</b>	switch(config)# <b>reload</b>	Copies the running configuration to the startup configuration.

The following example shows how to change the size of the RACL 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-configur 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 the error message you see when you set the ARP ACL TCAM value to a value other than 0 or 128, and then shows how to change the size of the ARP ACL TCAM region and verify the changes:

```
switch(config)# hardware profile tcam region arpacl 200
ARPACL size can be either 0 or 128
```

```
switch(config)# hardware profile tcam region arpacl 128
To start using ARPACL tcam, IFACL tcam size needs to be changed.
Changing IFACL tcam size to 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'
```

```
switch(config)# show hardware profile tcam region
sup size = 128
vacl size = 512
ifacl size = 256
qos size = 256
rbacl size = 0
span size = 128
racl size = 256
e-racl size = 512
e-vacl size = 512
qoslbl size = 512
ipsq size = 512
arpacl size = 128
switch(config)#
```

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

```
switch# configure sync
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-sync)# switch-profile s5010
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# hardware profile tcam region vacl 512
switch(config-sync-sp)# hardware profile tcam region e-vacl 512
switch(config-sync-sp)#
```

## Reverting to the Default TCAM Region Sizes

### SUMMARY STEPS

1. **configure terminal**
2. **switch(config)# no hardware profile tcam region**
3. (Optional) **copy running-config startup-config**
4. **switch(config)# reload**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config) #	Enters global configuration mode.
<b>Step 2</b>	<b>switch(config)# no hardware profile tcam region</b>	Reverts the configuration to the default ACL TCAM size.
<b>Step 3</b>	<b>copy running-config startup-config</b>  <b>Example:</b> switch(config) # copy running-config-startup-config switch(config) #	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.
<b>Step 4</b>	<b>switch(config)# reload</b>	Reloads the switch.

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

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

switch(config)# copy running-configur 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 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.

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **line vty**
3. switch(config-line)# **access-class access-list-number {in | out}**
4. (Optional) switch(config-line)# **no access-class access-list-number {in | out}**
5. switch(config-line)# **exit**
6. (Optional) switch# **show running-config aclmgr**
7. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>line vty</b>  <b>Example:</b> switch(config)# line vty switch(config-line)#	Enters line configuration mode.
<b>Step 3</b>	switch(config-line)# <b>access-class access-list-number {in   out}</b>  <b>Example:</b> switch(config-line)# access-class ozi2 in switch(config-line)#access-class ozi3 out switch(config)#	Specifies inbound or outbound access restrictions.
<b>Step 4</b>	switch(config-line)# <b>no access-class access-list-number {in   out}</b>  <b>Example:</b> switch(config-line)# no access-class ozi2 in switch(config-line)# no access-class ozi3 out switch(config)#	(Optional) Removes inbound or outbound access restrictions.

	Command or Action	Purpose
<b>Step 5</b>	switch(config-line)# <b>exit</b>  <b>Example:</b> switch(config-line)# exit switch#	Exits line configuration mode.
<b>Step 6</b>	switch# <b>show running-config aclmgr</b>  <b>Example:</b> switch# show running-config aclmgr	(Optional) Displays the running configuration of the ACLs on the switch.
<b>Step 7</b>	switch# <b>copy running-config startup-config</b>  <b>Example:</b> switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

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
<b>show running-config aclmgr</b>	Displays the running configuration of the ACLs configured on the switch.
<b>show users</b>	Displays the users that are connected.
<b>show access-lists <i>access-list-name</i></b>	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# conf t
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# conf t
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#
```

## Default ACL Settings

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

**Table 13: Default IP ACLs Parameters**

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

The following table lists the default settings for VACL parameters.

**Table 14: Default VACL Parameters**

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





## CHAPTER 8

# Configuring DHCP Snooping

---

This chapter describes how to configure Dynamic Host Configuration Protocol (DHCP) snooping on a Cisco NX-OS device.

- [Information About DHCP Snooping, page 107](#)
- [Information About the DHCP Relay Agent, page 109](#)
- [Guidelines and Limitations for DHCP Snooping, page 110](#)
- [Default Settings for DHCP Snooping, page 111](#)
- [Configuring DHCP Snooping, page 111](#)
- [Verifying the DHCP Snooping Configuration, page 120](#)
- [Displaying DHCP Bindings, page 120](#)
- [Clearing the DHCP Snooping Binding Database, page 121](#)
- [Configuration Examples for DHCP Snooping, page 122](#)

## 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 and do not disable the DHCP snooping feature.

### Global Enablement

After DHCP snooping is feature 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 received and using 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 may initiate traffic attacks or other hostile actions. To prevent such attacks, DHCP snooping filters messages from untrusted sources.

In an enterprise network, a trusted source is a 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 the Cisco Nexus 3000 Series switch, 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, all DHCP servers must be connected 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 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 agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently. By contrast, 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.



---

**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 instance (VRF) 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 that the devices adds to a DHCP request relayed to a different VRF includes the following:

### VPN identifier

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

### Link selection

Contains the subnet address of the interface that receives the DHCP request.

### Server identifier override

Contains the 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.

## 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 acting 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.

## Default Settings for DHCP Snooping

This table lists the default settings for DHCP snooping parameters.

**Table 15: 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

## Configuring DHCP Snooping

### Minimum DHCP Snooping Configuration

#### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	Enable the DHCP snooping feature.	When the DHCP snooping feature is disabled, you cannot configure DHCP snooping. For details, see <a href="#">Enabling or Disabling the DHCP Snooping Feature, on page 112</a> .
<b>Step 2</b>	Enable DHCP snooping globally.	For details, see <a href="#">Enabling or Disabling DHCP Snooping Globally, on page 113</a> .
<b>Step 3</b>	Enable DHCP snooping on at least one VLAN.	By default, DHCP snooping is disabled on all VLANs. For details, see <a href="#">Enabling or Disabling DHCP Snooping on a VLAN, on page 113</a> .

	Command or Action	Purpose
Step 4	Ensure that the DHCP server is connected to the switch using a trusted interface.	For details, see <a href="#">Configuring an Interface as Trusted or Untrusted</a> , on page 115.

## 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.

### SUMMARY STEPS

1. `config t`
2. `[no] feature dhcp`
3. `show running-config dhcp`
4. (Optional) `copy running-config startup-config`

### DETAILED STEPS

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

## 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. It preserves DHCP snooping configuration.

### Before You Begin

Ensure that you have enabled the DHCP snooping feature.

By default, DHCP snooping is globally disabled.

### SUMMARY STEPS

1. `config t`
2. `[no] ip dhcp snooping`
3. `show running-config dhcp`
4. (Optional) `copy running-config startup-config`

### DETAILED STEPS

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

## SUMMARY STEPS

1. `config t`
2. `[no] ip dhcp snooping vlan vlan-list`
3. `show running-config dhcp`
4. (Optional) `copy running-config startup-config`

## DETAILED STEPS

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

**SUMMARY STEPS**

1. `config t`
2. `[no] ip dhcp packet strict-validation`
3. `show running-config dhcp`
4. (Optional) `copy running-config startup-config`

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<code>config t</code>  <b>Example:</b> <code>switch# config t</code> <code>switch(config)#</code>	Enters global configuration mode.
<b>Step 2</b>	<code>[no] ip dhcp packet strict-validation</code>  <b>Example:</b> <code>switch(config)# ip dhcp packet strict-validation</code>	Enables the strict validation of DHCP packets by the DHCP snooping feature. The <b>no</b> option disables strict DHCP packet validation.
<b>Step 3</b>	<code>show running-config dhcp</code>  <b>Example:</b> <code>switch(config)# show running-config dhcp</code>	Shows the DHCP snooping configuration.
<b>Step 4</b>	<code>copy running-config startup-config</code>  <b>Example:</b> <code>switch(config)# copy running-config startup-config</code>	(Optional) 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.

## SUMMARY STEPS

1. `config t`
2. Do one of the following options.
  - `interface ethernet slot / port`
  - `interface port-channel channel-number`
3. `[no] ip dhcp snooping trust`
4. `show running-config dhcp`
5. (Optional) `copy running-config startup-config`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>config t</b>  <b>Example:</b> <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"> <li>• <code>interface ethernet slot / port</code></li> <li>• <code>interface port-channel channel-number</code></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	<ul style="list-style-type: none"> <li>• Enters interface configuration mode, where <i>slot / port</i> is the Layer 2 Ethernet interface that you want to configure as trusted or untrusted for DHCP snooping.</li> <li>• Enters interface configuration mode, where <i>slot / port</i> is the Layer 2 port-channel interface that you want to configure as trusted or untrusted for DHCP snooping.</li> </ul>
Step 3	<b>[no] ip dhcp snooping trust</b>  <b>Example:</b> <pre>switch(config-if)# ip dhcp snooping trust</pre>	Configures the interface as a trusted interface for DHCP snooping. The <b>no</b> option configures the port as an untrusted interface.
Step 4	<b>show running-config dhcp</b>  <b>Example:</b> <pre>switch(config-if)# show running-config dhcp</pre>	Shows the DHCP snooping configuration.
Step 5	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-if)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

## Enabling or Disabling the DHCP Relay Agent

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

### Before You Begin

Ensure that the DHCP feature is enabled.

### SUMMARY STEPS

1. `config t`
2. `[no] ip dhcp relay`
3. (Optional) `show ip dhcp relay`
4. (Optional) `show running-config dhcp`
5. (Optional) `copy running-config startup-config`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>config t</code>  <b>Example:</b> <code>switch# config t</code> <code>switch(config)#</code>	Enters global configuration mode.
Step 2	<code>[no] ip dhcp relay</code>  <b>Example:</b> <code>switch(config)# ip dhcp relay</code>	Enables the DHCP relay agent. The <b>no</b> option disables the DHCP relay agent.
Step 3	<code>show ip dhcp relay</code>  <b>Example:</b> <code>switch(config)# show ip dhcp relay</code>	(Optional) Displays the DHCP relay configuration.
Step 4	<code>show running-config dhcp</code>  <b>Example:</b> <code>switch(config)# show running-config dhcp</code>	(Optional) Displays the DHCP configuration.
Step 5	<code>copy running-config startup-config</code>  <b>Example:</b> <code>switch(config)# copy running-config startup-config</code>	(Optional) Copies 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.

### Before You Begin

You must enable Option 82 for the DHCP relay agent.

### SUMMARY STEPS

1. `config t`
2. `[no] ip dhcp relay information option vpn`
3. `[no] ip dhcp relay sub-option type cisco`
4. (Optional) `show ip dhcp relay`
5. (Optional) `show running-config dhcp`
6. (Optional) `copy running-config startup-config`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>config t</code>  <b>Example:</b> <code>switch# config t</code> <code>switch(config)#</code>	Enters global configuration mode.
Step 2	<code>[no] ip dhcp relay information option vpn</code>  <b>Example:</b> <code>switch(config)# ip dhcp relay information option vpn</code>	Enables VRF support for the DHCP relay agent. The <b>no</b> option disables this behavior.
Step 3	<code>[no] ip dhcp relay sub-option type cisco</code>  <b>Example:</b> <code>switch(config)# ip dhcp relay sub-option type cisco</code>	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 <b>no</b> option causes DHCP to use RFC numbers 5, 11, and 151 for the link selection, server ID override, and VRF name/VPN ID suboptions, respectively.
Step 4	<code>show ip dhcp relay</code>  <b>Example:</b> <code>switch(config)# show ip dhcp relay</code>	(Optional) Displays the DHCP relay configuration.
Step 5	<code>show running-config dhcp</code>  <b>Example:</b> <code>switch(config)# show running-config dhcp</code>	(Optional) Displays the DHCP configuration.

	Command or Action	Purpose
Step 6	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	(Optional) 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.

### SUMMARY STEPS

1. **config t**
2. **ip source binding** *IP-address MAC-address* **vlan** *vlan-id* {**interface ethernet** *slot/port* | **port-channel** *channel-no*}
3. (Optional) **show ip dhcp snooping binding**
4. (Optional) **show ip dhcp snooping binding dynamic**
5. (Optional) **copy running-config startup-config**

### DETAILED STEPS

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

	Command or Action	Purpose
<b>Step 4</b>	<b>show ip dhcp snooping binding dynamic</b>  <b>Example:</b> switch(config)# ip dhcp snooping binding dynamic	(Optional) Shows the DHCP snooping dynamic bindings.
<b>Step 5</b>	<b>copy running-config startup-config</b>  <b>Example:</b> switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

This 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 *Cisco Nexus 3000 Series NX-OS System Management Configuration Guide*.

Command	Purpose
<b>show running-config dhcp</b>	Displays the DHCP snooping configuration.
<b>show ip dhcp snooping</b>	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 *Cisco Nexus 3000 Series NX-OS System Management Configuration Guide*.

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.

## SUMMARY STEPS

1. (Optional) **clear ip dhcp snooping binding**
2. (Optional) **clear ip dhcp snooping binding interface ethernet** *slot/port*[*.subinterface-number*]
3. (Optional) **clear ip dhcp snooping binding interface port-channel** *channel-number*[*.subchannel-number*]
4. (Optional) **clear ip dhcp snooping binding vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface** {**ethernet** *slot/port*[*.subinterface-number*] | **port-channel** *channel-number*[*.subchannel-number*]} }
5. **show ip dhcp snooping binding**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>clear ip dhcp snooping binding</b>  <b>Example:</b> switch# clear ip dhcp snooping binding	(Optional) Clears all entries from the DHCP snooping binding database.
Step 2	<b>clear ip dhcp snooping binding interface ethernet</b> <i>slot/port</i> [ <i>.subinterface-number</i> ]  <b>Example:</b> switch# clear ip dhcp snooping binding interface ethernet 1/4	(Optional) Clears entries associated with a specific Ethernet interface from the DHCP snooping binding database.
Step 3	<b>clear ip dhcp snooping binding interface port-channel</b> <i>channel-number</i> [ <i>.subchannel-number</i> ]  <b>Example:</b> switch# clear ip dhcp snooping binding interface port-channel 72	(Optional) Clears entries associated with a specific port-channel interface from the DHCP snooping binding database.
Step 4	<b>clear ip dhcp snooping binding vlan</b> <i>vlan-id</i> <b>mac</b> <i>mac-address</i> <b>ip</b> <i>ip-address</i> <b>interface</b> { <b>ethernet</b> <i>slot/port</i> [ <i>.subinterface-number</i> ]   <b>port-channel</b> <i>channel-number</i> [ <i>.subchannel-number</i> ]} }  <b>Example:</b> switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface ethernet 2/11	(Optional) Clears a single, specific entry from the DHCP snooping binding database.

	Command or Action	Purpose
Step 5	<b>show ip dhcp snooping binding</b>  <b>Example:</b> switch# show ip dhcp snooping binding	Displays the DHCP snooping binding database.

## Configuration Examples for DHCP Snooping

This 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 Dynamic ARP Inspection

---

This chapter describes how to configure dynamic Address Resolution Protocol (ARP) inspection (DAI) on a Cisco Nexus 3000 Series switch.

This chapter includes the following sections:

- [Information About DAI, page 123](#)
- [Licensing Requirements for DAI, page 127](#)
- [Prerequisites for DAI, page 127](#)
- [Guidelines and Limitations for DAI, page 127](#)
- [Default Settings for DAI, page 128](#)
- [Configuring DAI, page 129](#)
- [Verifying the DAI Configuration, page 134](#)
- [Monitoring and Clearing DAI Statistics, page 135](#)
- [Configuration Examples for DAI, page 135](#)

## Information About DAI

### Understanding ARP

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, host B wants to send information to host A but does not have the MAC address of host A in its ARP cache. In ARP terms, host B is the sender and host A is the target.

To get the MAC address of host A, host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of host A. All hosts within the broadcast domain receive the ARP request, and host A responds with its MAC address.

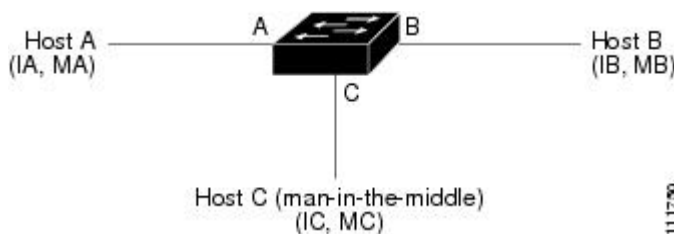
## Understanding ARP Spoofing Attacks

ARP spoofing attacks and ARP cache poisoning can occur because ARP allows a reply from a host even if an ARP request was not received. After the attack, all traffic from the device under attack flows through the attacker's computer and then to the router, switch, or host.

An ARP spoofing attack can affect hosts, switches, and routers connected to your Layer 2 network by sending false information to the ARP caches of the devices connected to the subnet. Sending false information to an ARP cache is known as ARP cache poisoning. Spoof attacks can also intercept traffic intended for other hosts on the subnet.

This figure shows an example of ARP cache poisoning.

**Figure 4: ARP Cache Poisoning**



Hosts A, B, and C are connected to the device on interfaces A, B, and C, all of which are on the same subnet. Their IP and MAC addresses are shown in parentheses; for example, host A uses IP address IA and MAC address MA. When host A needs to send IP data to host B, it broadcasts an ARP request for the MAC address associated with IP address IB. When the device and host B receive the ARP request, they populate their ARP caches with an ARP binding for a host with the IP address IA and a MAC address MA; for example, IP address IA is bound to MAC address MA. When host B responds, the device and host A populate their ARP caches with a binding for a host with the IP address IB and the MAC address MB.

Host C can poison the ARP caches of the device, host A, and host B by broadcasting two forged ARP responses with bindings: one for a host with an IP address of IA and a MAC address of MC and another for a host with the IP address of IB and a MAC address of MC. Host B and the device then use the MAC address MC as the destination MAC address for traffic intended for IA, which means that host C intercepts that traffic. Likewise, host A and the device use the MAC address MC as the destination MAC address for traffic intended for IB.

Because host C knows the true MAC addresses associated with IA and IB, it can forward the intercepted traffic to those hosts by using the correct MAC address as the destination. This topology, in which host C has inserted itself into the traffic stream from host A to host B, is an example of a *man-in-the middle* attack.

## Understanding DAI and ARP Spoofing Attacks

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

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

DAI can determine the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a Dynamic Host Configuration Protocol (DHCP) snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the device. It can also contain static entries that you create. If the ARP packet is received on a trusted interface, the device forwards the packet without any checks. On untrusted interfaces, the device forwards the packet only if it is valid.

You can configure DAI to drop ARP packets when the IP addresses in the packets are invalid or when the MAC addresses in the body of the ARP packets do not match the addresses specified in the Ethernet header.

## Interface Trust States and Network Security

DAI associates a trust state with each interface on the device. Packets that arrive on trusted interfaces bypass all DAI validation checks, and packets that arrive on untrusted interfaces go through the DAI validation process.

In a typical network configuration, the guidelines for configuring the trust state of interfaces are as follows:

### Untrusted

Interfaces that are connected to hosts

### Trusted

Interfaces that are connected to devices

With this configuration, all ARP packets that enter the network from a device bypass the security check. No other validation is needed at any other place in the VLAN or in the network.



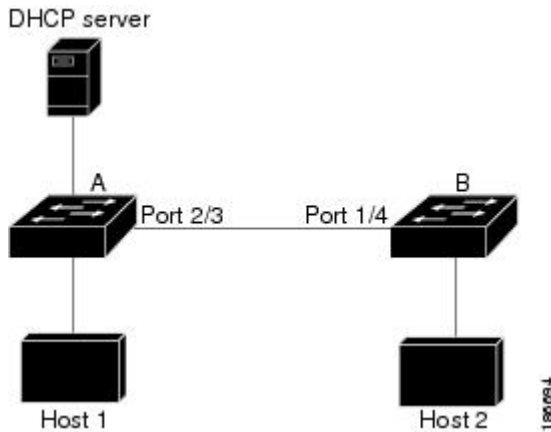
#### Caution

---

Use the trust state configuration carefully. Configuring interfaces as untrusted when they should be trusted can result in a loss of connectivity.

---

In this figure, assume that both device A and device B are running DAI on the VLAN that includes host 1 and host 2. If host 1 and host 2 acquire their IP addresses from the DHCP server connected to device A, only device A binds the IP-to-MAC address of host 1. If the interface between device A and device B is untrusted, the ARP packets from host 1 are dropped by device B and connectivity between host 1 and host 2 is lost.

**Figure 5: ARP Packet Validation on a VLAN Enabled for DAI**

If you configure interfaces as trusted when they should be untrusted, you may open a security hole in a network. If device A is not running DAI, host 1 can easily poison the ARP cache of device B (and host 2, if you configured the link between the devices as trusted). This condition can occur even though device B is running DAI.

DAI ensures that hosts (on untrusted interfaces) connected to a device that runs DAI do not poison the ARP caches of other hosts in the network; however, DAI does not prevent hosts in other portions of the network from poisoning the caches of the hosts that are connected to a device that runs DAI.

If some devices in a VLAN run DAI and other devices do not, then the guidelines for configuring the trust state of interfaces on a device running DAI becomes the following:

#### Untrusted

Interfaces that are connected to hosts or to devices that *are not* running DAI

#### Trusted

Interfaces that are connected to devices that *are* running DAI

To validate the bindings of packets from devices that are not running DAI, configure ARP ACLs on the device running DAI. When you cannot determine the bindings, isolate at Layer 3 the devices that run DAI from devices that do not run DAI.



**Note** Depending on your network setup, you may not be able to validate a given ARP packet on all devices in the VLAN.

## Logging DAI Packets

Cisco NX-OS maintains a buffer of log entries about DAI packets processed. Each log entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.

You can also specify the type of packets that are logged. By default, a Cisco NX-OS device logs only packets that DAI drops.

If the log buffer overflows, the device overwrites the oldest DAI log entries with newer entries. You can configure the maximum number of entries in the buffer.

**Note**

Cisco NX-OS does not generate system messages about DAI packets that are logged.

## Licensing Requirements for DAI

This table shows the licensing requirements for DAI.

Product	License Requirement
Cisco NX-OS	DAI 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> .

## Prerequisites for DAI

DAI has the following prerequisite:

- You must enable the DHCP feature before you can configure DAI.

## Guidelines and Limitations for DAI

DAI has the following configuration guidelines and limitations:

- DAI is an ingress security feature; it does not perform any egress checking.
- DAI is not effective for hosts connected to devices that do not support DAI or that do not have this feature enabled. Because man-in-the-middle attacks are limited to a single Layer 2 broadcast domain, you should separate the domain with DAI from domains without DAI. This separation secures the ARP caches of hosts in the domain with DAI.
- DAI depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. If you want DAI to use static IP-MAC address bindings to determine if ARP packets are valid, DHCP snooping needs only to be enabled. If you want DAI to use dynamic IP-MAC address bindings to determine if ARP packets are valid, DHCP snooping must be configured on the same VLANs on which you configure DAI.
- When you use the **feature dhcp** command to enable the DHCP feature, there is a delay of approximately 30 seconds before the I/O modules receive the DHCP or DAI configuration. This delay occurs regardless of the method that you use to change from a configuration with the DHCP feature disabled to a

configuration with the DHCP feature enabled. For example, if you use the Rollback feature to revert to a configuration that enables the DHCP feature, the I/O modules receive the DHCP and DAI configuration approximately 30 seconds after you complete the rollback.

- DAI is supported on access ports, trunk ports, port-channel ports, and private VLAN ports.
- The DAI trust configuration of a port channel determines the trust state of all physical ports that you assign to the port channel. For example, if you have configured a physical port as a trusted interface and then you add that physical port to a port channel that is an untrusted interface, the physical port becomes untrusted.
- When you remove a physical port from a port channel, the physical port does not retain the DAI trust state configuration of the port channel.
- When you change the trust state on the port channel, the device configures a new trust state on all the physical ports that comprise the channel.
- If you want DAI to use static IP-MAC address bindings to determine if ARP packets are valid, ensure that DHCP snooping is enabled and that you have configured the static IP-MAC address bindings.
- If you want DAI to use dynamic IP-MAC address bindings to determine if ARP packets are valid, ensure that DHCP snooping is enabled.

## Default Settings for DAI

This table lists the default settings for DAI parameters.

**Table 16: Default DAI Parameters**

Parameters	Default
DAI	Disabled on all VLANs.
Interface trust state	All interfaces are untrusted.
Validation checks	No checks are performed.
Log buffer	When DAI is enabled, all denied or dropped ARP packets are logged. The number of entries in the log is 32. The number of system messages is limited to 5 per second. The logging-rate interval is 1 second.
Per-VLAN logging	All denied or dropped ARP packets are logged.

# Configuring DAI

## Enabling or Disabling DAI on VLANs

You can enable or disable DAI on VLANs. By default, DAI is disabled on all VLANs.

### Before You Begin

If you are enabling DAI, ensure the following:

- Ensure that the DHCP feature is enabled.
- The VLANs on which you want to enable DAI are configured.

### SUMMARY STEPS

1. **configure terminal**
2. **[no] ip arp inspection vlan *list***
3. (Optional) **show ip arp inspection vlan *list***
4. (Optional) **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ip arp inspection vlan <i>list</i></b>  <b>Example:</b> switch(config)# ip arp inspection vlan 13	Enables DAI for the specified list of VLANs. The <b>no</b> option disables DAI for the specified VLANs.
<b>Step 3</b>	<b>show ip arp inspection vlan <i>list</i></b>  <b>Example:</b> switch(config)# show ip arp inspection vlan 13	(Optional) Shows the DAI status for the specified list of VLANs.
<b>Step 4</b>	<b>copy running-config startup-config</b>  <b>Example:</b> switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

## Configuring the DAI Trust State of a Layer 2 Interface

You can configure the DAI interface trust state of a Layer 2 interface. By default, all interfaces are untrusted.

A device forwards ARP packets that it receives on a trusted Layer 2 interface but does not check them.

On untrusted interfaces, the device intercepts all ARP requests and responses, verifies that the intercepted packets have valid IP-MAC address bindings before updating the local cache and forwarding the packet to the appropriate destination. If the device determines that packets have invalid bindings, it drops the packets and logs them according to the logging configuration.

### Before You Begin

If you are enabling DAI, ensure that the DHCP feature is enabled.

### SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot / number*
3. **[no] ip arp inspection trust**
4. (Optional) **show ip arp inspection interface** *type slot / number*
5. (Optional) **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>type slot / number</i>  <b>Example:</b> switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode.
<b>Step 3</b>	<b>[no] ip arp inspection trust</b>  <b>Example:</b> switch(config-if)# ip arp inspection trust	Configures the interface as a trusted ARP interface. The <b>no</b> option configures the interface as an untrusted ARP interface.
<b>Step 4</b>	<b>show ip arp inspection interface</b> <i>type slot / number</i>  <b>Example:</b> switch(config-if)# show ip arp inspection interface ethernet 2/1	(Optional) Displays the trust state and the ARP packet rate for the specified interface.

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

## Enabling or Disabling Additional Validation

You can enable or disable additional validation of ARP packets. By default, no additional validation of ARP packets is enabled. When no additional validation is configured, the source MAC address, source IP address check against the IP-to-MAC binding entry for ARP packets is done using the Ethernet source MAC address (not the ARP sender MAC address) and the ARP sender IP address.

DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. You can enable additional validation on the destination MAC address, the sender and target IP addresses, and the source MAC address.

You can use the following keywords with the **ip arp inspection validate** command to implement additional validations:

### **dst-mac**

Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

### **ip**

Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

### **src-mac**

Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body for ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

When enabling additional validation, follow these guidelines:

- You must specify at least one of the keywords. You can specify one, two, or all three keywords.
- Each **ip arp inspection validate** command that you enter replaces the configuration from any previous commands. If you enter an **ip arp inspection validate** command to enable src-mac and dst-mac validations, and a second **ip arp inspection validate** command to enable ip validation, the src-mac and dst-mac validations are disabled when you enter the second command.

**SUMMARY STEPS**

1. **configure terminal**
2. **[no] ip arp inspection validate** {[src-mac] [dst-mac] [ip]}
3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ip arp inspection validate</b> {[src-mac] [dst-mac] [ip]}  <b>Example:</b> switch(config)# ip arp inspection validate src-mac dst-mac ip	Enables additional DAI validation, or if you use the <b>no</b> option, disables additional DAI validation.
<b>Step 3</b>	<b>show running-config dhcp</b>  <b>Example:</b> switch(config)# show running-config dhcp	(Optional) Displays the DHCP snooping configuration, including the DAI configuration.
<b>Step 4</b>	<b>copy running-config startup-config</b>  <b>Example:</b> switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

**Configuring the DAI Logging Buffer Size**

You can configure the DAI logging buffer size. The default buffer size is 32 messages.

**SUMMARY STEPS**

1. **configure terminal**
2. **[no] ip arp inspection log-buffer entries** *number*
3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	<b>[no] ip arp inspection log-buffer entries <i>number</i></b>  <b>Example:</b> <pre>switch(config)# ip arp inspection log-buffer entries 64</pre>	Configures the DAI logging buffer size. The <b>no</b> option reverts to the default buffer size, which is 32 messages. The buffer size can be between 0 and 2048 messages.
Step 3	<b>show running-config dhcp</b>  <b>Example:</b> <pre>switch(config)# show running-config dhcp</pre>	(Optional) Displays the DHCP snooping configuration, including the DAI configuration.
Step 4	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

## Configuring DAI Log Filtering

You can configure how the device determines whether to log a DAI packet. By default, the device logs DAI packets that are dropped.

## SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
  - **ip arp inspection vlan *vlan-list* logging dhcp-bindings all**
  - **ip arp inspection vlan *vlan-list* logging dhcp-bindings none**
  - **ip arp inspection vlan *vlan-list* logging dhcp-bindings permit**
  - **no ip arp inspection vlan *vlan-list* logging dhcp-bindings {all | none | permit}**
3. (Optional) **show running-config dhcp**
4. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> <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"> <li>• <b>ip arp inspection vlan <i>vlan-list</i> logging dhcp-bindings all</b></li> <li>• <b>ip arp inspection vlan <i>vlan-list</i> logging dhcp-bindings none</b></li> <li>• <b>ip arp inspection vlan <i>vlan-list</i> logging dhcp-bindings permit</b></li> <li>• <b>no ip arp inspection vlan <i>vlan-list</i> logging dhcp-bindings {all   none   permit}</b></li> </ul> <b>Example:</b> <pre>switch(config)# ip arp inspection vlan 100 dhcp-bindings permit</pre>	Configures DAI log filtering, as follows. The <b>no</b> option removes DAI log filtering. <ul style="list-style-type: none"> <li>• Logs all packets that match DHCP bindings.</li> <li>• Does not log packets that match DHCP bindings.</li> <li>• Logs packets permitted by DHCP bindings.</li> <li>• Removes DAI log filtering.</li> </ul>
Step 3	<b>show running-config dhcp</b>  <b>Example:</b> <pre>switch(config)# show running-config dhcp</pre>	(Optional) Displays the DHCP snooping configuration, including the DAI configuration.
Step 4	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

## Verifying the DAI Configuration

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

Command	Purpose
<b>show running-config arp</b>	Displays DAI configuration.
<b>show ip arp inspection</b>	Displays the status of DAI.
<b>show ip arp inspection interface ethernet</b>	Displays the trust state and ARP packet rate for a specific interface.

Command	Purpose
<code>show ip arp inspection vlan</code>	Displays the DAI configuration for a specific VLAN.
<code>show arp access-lists</code>	Displays ARP ACLs.
<code>show ip arp inspection log</code>	Displays the DAI log configuration.

## Monitoring and Clearing DAI Statistics

To monitor and clear DAI statistics, use the commands in this table. For more information about these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Command	Purpose
<code>show ip arp inspection statistics</code>	Displays DAI statistics.
<code>show ip arp ethernet</code>	Displays interface-specific DAI statistics.
<code>clear ip arp inspection statistics</code>	Clears DAI statistics.

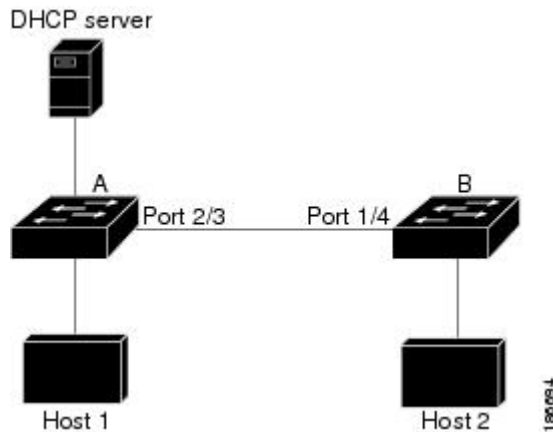
## Configuration Examples for DAI

### Example 1 Two Devices Support DAI

These procedures show how to configure DAI when two devices support DAI.

This figure shows the network configuration for this example. Host 1 is connected to device A, and Host 2 is connected to device B. Both devices are running DAI on VLAN 1 where the hosts are located. A DHCP server is connected to device A. Both hosts acquire their IP addresses from the same DHCP server. Device A has the bindings for Host 1 and Host 2, and device B has the binding for Host 2. Device A Ethernet interface 2/3 is connected to the device B Ethernet interface 1/4.

Figure 6: Two Devices Supporting DAI



DAI depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically-assigned IP addresses.

- This configuration does not work if the DHCP server is moved from device A to a different location.
- To ensure that this configuration does not compromise security, configure Ethernet interface 2/3 on device A and Ethernet interface 1/4 on device B as trusted.

## Configuring Device A

To enable DAI and configure Ethernet interface 2/3 on device A as trusted, follow these steps:

**Step 1** While logged into device A, verify the connection between device A and device B.

**Example:**

```
switchA# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device ID         Local Intrfce  Hldtme  Capability  Platform      Port ID
switchB           Ethernet2/3    177     R S I       WS-C2960-24TC Ethernet1/4
switchA#
```

**Step 2** Enable DAI on VLAN 1 and verify the configuration.

**Example:**

```
switchA# config t
switchA(config)# ip arp inspection vlan 1
switchA(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----
Configuration              : Enabled
```

```
Operation State : Active
switchA(config)#
```

**Step 3** Configure Ethernet interface 2/3 as trusted.

**Example:**

```
switchA(config)# interface ethernet 2/3
switchA(config-if)# ip arp inspection trust
switchA(config-if)# exit
switchA(config)# exit
switchA# show ip arp inspection interface ethernet 2/3
Interface      Trust State   Rate (pps)   Burst Interval
-----
Ethernet2/3    Trusted       15           5
```

**Step 4** Verify the bindings.

**Example:**

```
switchA# show ip dhcp snooping binding
MacAddress      IpAddress      LeaseSec      Type           VLAN   Interface
-----
00:60:0b:00:12:89  10.0.0.1      0             dhcp-snooping  1      Ethernet2/3
switchA#
```

**Step 5** Check the statistics before and after DAI processes any packets.

**Example:**

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded = 0
ARP Res Forwarded = 0
ARP Req Dropped   = 0
ARP Res Dropped   = 0
DHCP Drops        = 0
DHCP Permits      = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req  = 0
IP Fails-ARP Res  = 0
switchA#
```

If Host 1 sends out two ARP requests with an IP address of 10.0.0.1 and a MAC address of 0002.0002.0002, both requests are permitted, shown as follows:

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded = 2
ARP Res Forwarded = 0
ARP Req Dropped   = 0
ARP Res Dropped   = 0
DHCP Drops        = 0
DHCP Permits      = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req  = 0
IP Fails-ARP Res  = 0
```

If Host 1 tries to send an ARP request with an IP address of 10.0.0.3, the packet is dropped and an error message is logged.

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Ethernet2/3, vlan
1. ([0002.0002.0002/10.0.0.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Fri Jul 13 2008])
```

## Example 1 Two Devices Support DAI

The statistics display as follows:

```
switchA# show ip arp inspection statistics vlan 1
switchA#
Vlan : 1
-----
ARP Req Forwarded = 2
ARP Res Forwarded = 0
ARP Req Dropped   = 2
ARP Res Dropped   = 0
DHCP Drops        = 2
DHCP Permits      = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

## Configuring Device B

To enable DAI and configure Ethernet interface 1/4 on device B as trusted, follow these steps:

**Step 1** While logged into device B, verify the connection between device B and device A.

**Example:**

```
switchB# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device ID         Local Intrfce  Hldtme  Capability  Platform  Port ID
switchA           Ethernet1/4    120     R S I       WS-C2960-24TC  Ethernet2/3
switchB#
```

**Step 2** Enable DAI on VLAN 1, and verify the configuration.

**Example:**

```
switchB# config t
switchB(config)# ip arp inspection vlan 1
switchB(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----
Configuration      : Enabled
Operation State    : Active
switchB(config)#
```

**Step 3** Configure Ethernet interface 1/4 as trusted.

**Example:**

```
switchB(config)# interface ethernet 1/4
switchB(config-if)# ip arp inspection trust
switchB(config-if)# exit
switchB(config)# exit
switchB# show ip arp inspection interface ethernet 1/4
Interface      Trust State  Rate (pps)  Burst Interval
```

```
-----
Ethernet1/4      Trusted          15              5
switchB#
```

**Step 4** Verify the list of DHCP snooping bindings.

**Example:**

```
switchB# show ip dhcp snooping binding
-----
MacAddress      IpAddress      LeaseSec      Type          VLAN  Interface
-----
00:01:00:01:00:01  10.0.0.2      4995         dhcp-snooping  1    Ethernet1/4
switchB#
```

**Step 5** Check the statistics before and after DAI processes any packets.

**Example:**

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded = 0
ARP Res Forwarded = 0
ARP Req Dropped   = 0
ARP Res Dropped   = 0
DHCP Drops        = 0
DHCP Permits      = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req  = 0
IP Fails-ARP Res  = 0
switchB#
```

If Host 2 sends out an ARP request with the IP address 10.0.0.2 and the MAC address 0001.0001.0001, the packet is forwarded and the statistics are updated.

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded = 1
ARP Res Forwarded = 0
ARP Req Dropped   = 0
ARP Res Dropped   = 0
DHCP Drops        = 0
DHCP Permits      = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req  = 0
IP Fails-ARP Res  = 0
switchB#
```

If Host 2 attempts to send an ARP request with the IP address 10.0.0.1, DAI drops the request and logs the following system message:

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Ethernet1/4, vlan
1. ([0001.0001.0001/10.0.0.1/0000.0000.0000/0.0.0.0/01:53:21 UTC Fri Jun 13 2008])
```

The statistics display as follows:

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded = 1
ARP Res Forwarded = 0
ARP Req Dropped   = 1
ARP Res Dropped   = 0
DHCP Drops        = 1
DHCP Permits      = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
```

## Example 1 Two Devices Support DAI

```
IP Fails-ARP Req  = 0
IP Fails-ARP Res  = 0
switchB#
```

---



# 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](#), page 141
- [Licensing Requirements for Unicast RPF](#), page 143
- [Guidelines and Limitations for Unicast RPF](#), page 143
- [Default Settings for Unicast RPF](#), page 144
- [Configuring Unicast RPF](#), page 144
- [Configuration Examples for Unicast RPF](#), page 146
- [Verifying Unicast RPF Configuration](#), page 147

## 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 or IPv6 addresses to allow attackers to thwart efforts to locate or filter the attacks. Unicast RPF deflects attacks by forwarding only the packets that have source addresses that are valid and consistent with the IP routing table.

When you enable Unicast RPF on an interface, the 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 Process

Unicast RPF has several key implementation principles:

- The packet must be received at an interface that has the best return path (route) to the packet source (a process called *symmetric routing*). There must be a route in the FIB that matches the route to the receiving interface. Static routes, network statements, and dynamic routing add routes to the FIB.
- IP source addresses at the receiving interface must match the routing entry for the interface.
- Unicast RPF is an input function and is applied only on the input interface of a device at the upstream end of a connection.

You can use Unicast RPF for downstream networks, even if the downstream network has other connections to the Internet.

**Caution**

---

Be careful when using optional BGP attributes, such as weight and local preference, because an attacker can modify the best path back to the source address. Modification would affect the operation of Unicast RPF.

---

When a packet is received at the interface where you have configured Unicast RPF and ACLs, the Cisco NX-OS software performs the following actions:

### SUMMARY STEPS

1. Checks the input ACLs on the inbound interface.
2. Uses Unicast RPF to verify that the packet has arrived on the best return path to the source, which it does by doing a reverse lookup in the FIB table.
3. Conducts a FIB lookup for packet forwarding.
4. Checks the output ACLs on the outbound interface.
5. Forwards the packet.

## DETAILED STEPS

- 
- Step 1** Checks the input ACLs on the inbound interface.
- Step 2** Uses Unicast RPF to verify that the packet has arrived on the best return path to the source, which it does by doing a reverse lookup in the FIB table.
- Step 3** Conducts a FIB lookup for packet forwarding.
- Step 4** Checks the output ACLs on the outbound interface.
- Step 5** Forwards the packet.
- 

## Global Statistics

Each time the Cisco NX-OS device drops a packet at an interface due to a failed unicast RPF check, that information is counted globally on the device on a per-forwarding engine (FE) basis. Global statistics on dropped packets provide information about potential attacks on the network, but they do not specify which interface is the source of the attack. Per-interface statistics on packets dropped due to a failed unicast RPF check are not available.

## 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:

- 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.
- Unicast RPF allows packets with 0.0.0.0 source and 255.255.255.255 destination to pass so that the Bootstrap Protocol (BOOTP) and the Dynamic Host Configuration Protocol (DHCP) can operate correctly.

**Note**

If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

## Default Settings for Unicast RPF

This table lists the default settings for Unicast RPF parameters.

**Table 17: 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.

### SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet *slot/port***
3. **ip verify unicast source reachable-via {any [allow-default] | rx}**
4. **ipv6 verify unicast source reachable-via {any [allow-default] | rx}**
5. **exit**
6. (Optional) **show ip interface ethernet *slot/port***
7. (Optional) **show running-config interface ethernet *slot/port***
8. (Optional) **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	<b>interface ethernet <i>slot/port</i></b>  <b>Example:</b> <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	Specifies an Ethernet interface and enters interface configuration mode.
Step 3	<b>ip verify unicast source reachable-via {any [allow-default]   rx}</b>  <b>Example:</b> <pre>switch(config-if)# ip verify unicast source reachable-via any</pre>	<p>Configures Unicast RPF on the interface for IPv4.</p> <p>The <b>any</b> keyword specifies loose Unicast RPF.</p> <p>If you specify the <b>allow-default</b> keyword, the source address lookup can match the default route and use that for verification.</p> <p>The <b>rx</b> keyword specifies strict Unicast RPF.</p>
Step 4	<b>ipv6 verify unicast source reachable-via {any [allow-default]   rx}</b>  <b>Example:</b> <pre>switch(config-if)# ipv6 verify unicast source reachable-via any</pre>	<p>Configures Unicast RPF on the interface for IPv6.</p> <p>The <b>any</b> keyword specifies loose Unicast RPF.</p> <p>If you specify the <b>allow-default</b> keyword, the source address lookup can match the default route and use that for verification.</p> <p>The <b>rx</b> keyword specifies strict Unicast RPF.</p>

	Command or Action	Purpose
Step 5	<b>exit</b>  <b>Example:</b> switch(config-cmap)# exit switch(config)#	Exits class map configuration mode.
Step 6	<b>show ip interface ethernet <i>slot/port</i></b>  <b>Example:</b> switch(config)# show ip interface ethernet 2/3	(Optional) Displays the IP information for an interface.
Step 7	<b>show running-config interface ethernet <i>slot/port</i></b>  <b>Example:</b> switch(config)# show running-config interface ethernet 2/3	(Optional) Displays the configuration for an interface in the running configuration.
Step 8	<b>copy running-config startup-config</b>  <b>Example:</b> switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

## Configuration Examples for Unicast RPF

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

```
interface Ethernet2/3
 ip address 172.23.231.240/23
 ip verify unicast source reachable-via any
```

The following example shows how to configure strict Unicast RFP for IPv4 packets:

```
interface Ethernet2/2
 ip address 172.23.231.240/23
 ip verify unicast source reachable-via rx
```

The following example shows how to configure loose Unicast RFP for IPv6 packets:

```
interface Ethernet2/1
 ipv6 address 2001:0DB8:c18:1::3/64
 ipv6 verify unicast source reachable-via any
```

The following example shows how to configure strict Unicast RFP for IPv6 packets:

```
interface Ethernet2/4
 ipv6 address 2001:0DB8:c18:1::3/64
 ipv6 verify unicast source reachable-via rx
```

## Verifying Unicast RPF Configuration

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

Command	Purpose
<b>show running-config interface ethernet <i>slot/port</i></b>	Displays the interface configuration in the running configuration.
<b>show running-config ip [all]</b>	Displays the IPv4 configuration in the running configuration.
<b>show startup-config interface ethernet <i>slot/port</i></b>	Displays the interface configuration in the startup configuration.
<b>show startup-config ip</b>	Displays the IP configuration in the startup configuration.





## CHAPTER 11

# Configuring Control Plane Policing

---

This chapter describes how to configure Control Plane Policing (CoPP) on a Cisco NX-OS device.

This chapter includes the following sections:

- [Information About CoPP, page 149](#)
- [Licensing Requirements for CoPP, page 156](#)
- [Guidelines and Limitations for CoPP, page 156](#)
- [Configuring CoPP, page 157](#)
- [CoPP Show Commands, page 161](#)
- [Displaying the CoPP Configuration Status, page 162](#)
- [Monitoring CoPP, page 162](#)
- [Clearing the CoPP Statistics, page 163](#)
- [CoPP Configuration Examples, page 163](#)
- [Sample CoPP Configuration, page 164](#)
- [Example: Changing or Reapplying the Default CoPP Policy Using the Setup Utility, page 167](#)
- [Additional References for CoPP, page 167](#)
- [Feature History for CoPP, page 168](#)

## Information About CoPP

Control Plane Policing (CoPP) protects the control plane and separates it from the data plane, thereby ensuring 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. Attacks on the supervisor module can be of various types such as DoS that generates IP traffic streams to the control plane at a very high rate. These attacks force the control plane to spend a large amount of time in handling these packets and prevents 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 setting appropriate control plane protection.

---

## Control Plane Protection

To protect the control plane, the Cisco NX-OS device segregates different packets destined to 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, then 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 like 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 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.



### Important

If you are upgrading from an NX-OS release which does not support the CoPP feature, the setup utility must be explicitly run to enable CoPP on the device after the upgrade. Not configuring CoPP protection can leave your NX-OS device vulnerable to DoS attacks.

## Default CoPP Policy

This policy is applied to the switch by default. It has the classes with policer rates that should suit most network installations. You cannot modify this policy or the class maps associated with it. In addition, you cannot modify the class map configurations in this policy.

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy-default
```

```
class copp-s-default
  police pps 400
class copp-s-l2switched
  police pps 200
class copp-s-ping
  police pps 100
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-s-l3destmiss
  police pps 100
class copp-s-glean
  police pps 500
class copp-s-selfIp
  police pps 500
class copp-s-mtufail
  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 1000
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-icmp
  police pps 200
class copp-s-bpdu
  police pps 12000
class copp-s-tacacsradius
  police pps 400
class copp-s-stftp
  police pps 400
```

## Layer 2 CoPP Policy

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-l2switched
    police pps 200
  class copp-s-ping
    police pps 100
  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-s-l3destmiss
  police pps 100
class copp-s-glean
  police pps 500
class copp-s-selfIp
  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-decpresp
  police pps 300
class copp-s-dai
  police pps 300
class copp-s-igmp
  police pps 400
class copp-s-routingproto2
  police pps 900
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 900
class copp-s-arp
  police pps 200
class copp-s-icmp
  police pps 200
class copp-s-bpdu
  police pps 12200
class copp-s-tacacsradius
  police pps 400
class copp-s-stftp
  police pps 400

```

## Layer 3 CoPP Policy

This policy has the following configuration:

```

policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-l2switched
    police pps 200
  class copp-s-ping
    police pps 100
  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-s-l3destmiss
  police pps 100

```

```
class copp-s-glean
  police pps 500
class copp-s-selfIp
  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 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-icmp
  police pps 200
class copp-s-bpdu
  police pps 6000
class copp-tacacsradius
  police pps 400
class copp-stftp
  police pps 400
```

## 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 specific to their requirements.



---

**Note**

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

ACLs can be associated with both static and dynamic classes.

---

## CoPP Configuration Information

Only a single ACL ( with multiple ACEs within it ) can be associated with a given class. Multiple ACLs per class is not supported.

The creation of new policy-maps is not supported. An existing policy can be tuned for new classes as well as for policing rate of existing classes.

The maximum number of TCAM entries for CoPP ACLs is capped to 64.

ACLs can be associated with both static and dynamic classes.

## 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

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	CoPP 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 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.

- Customizing CoPP is an ongoing process. CoPP must be configured according to the protocols and features used in your specific environment as well as the supervisor features that are required by the server environment. As these protocols and features change, CoPP must be modified.
- Cisco recommends that you continuously monitor CoPP. If drops occur, determine if CoPP dropped traffic unintentionally or in response to a malfunction or attack. In either event, analyze the situation and evaluate the need to use a different CoPP policy or modify the customized CoPP policy.
- 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.

## 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.

You can configure policies for IPv4 or IPv6 packets.

#### Before You Begin

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

#### SUMMARY STEPS

1. **configure terminal**
2. **class-map type control-plane match-any** *class-map-name*
3. (Optional) **match access-group name** *access-list-name*
4. **exit**
5. (Optional) **show class-map type control-plane** [*class-map-name*]
6. (Optional) **copy running-config startup-config**

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	<b>class-map type control-plane match-any</b> <i>class-map-name</i>	Specifies a control plane class map and enters class map configuration mode. The default class matching is match-any.

	Command or Action	Purpose
	<p><b>Example:</b>  <pre>switch(config)# class-map type control-plane ClassMapA switch(config-cmap)#</pre></p>	<p>The name can be a maximum of 64 characters long and is case sensitive.</p> <p><b>Note</b> You cannot use class-default, match-all, or match-any as class map names.</p>
<b>Step 3</b>	<p><b>match access-group name</b> <i>access-list-name</i></p> <p><b>Example:</b>  <pre>switch(config-cmap)# match access-group name MyAccessList</pre></p>	<p>(Optional)  Specifies matching for an IP ACL. You can repeat this step to match more than one IP ACL.</p> <p><b>Note</b> The permit and deny ACL keywords are ignored in the CoPP matching.</p>
<b>Step 4</b>	<p><b>exit</b></p> <p><b>Example:</b>  <pre>switch(config-cmap)# exit switch(config)#</pre></p>	<p>Exits class map configuration mode.</p>
<b>Step 5</b>	<p><b>show class-map type control-plane</b> [<i>class-map-name</i>]</p> <p><b>Example:</b>  <pre>switch(config)# show class-map type control-plane</pre></p>	<p>(Optional)  Displays the control plane class map configuration.</p>
<b>Step 6</b>	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b>  <pre>switch(config)# copy running-config startup-config</pre></p>	<p>(Optional)  Copies the running configuration to the startup configuration.</p>

## Configuring a Control Plane Policy Map

You must configure a policy map for CoPP, which include policing parameters. If you do not configure a policer for a class, then 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.

## SUMMARY STEPS

1. **configure terminal**
2. **policy-map type control-plane** *policy-map-name*
3. **class** {*class-map-name* [**insert-before** *class-map-name2*] | **class**}
4. **police** [**pps**] {*pps-value*}
5. **exit**
6. **exit**
7. (Optional) **show policy-map type control-plane** [**expand**] [**name** *class-map-name*]
8. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>policy-map type control-plane</b> <i>policy-map-name</i>  <b>Example:</b> switch(config)# policy-map type control-plane ClassMapA switch(config-pmap)#	Specifies a control plane policy map and enters policy map configuration mode. The policy map name can have a maximum of 64 characters and is case sensitive.
<b>Step 3</b>	<b>class</b> { <i>class-map-name</i> [ <b>insert-before</b> <i>class-map-name2</i> ]   <b>class</b> }	Specifies a control plane class map name or the class default and enters control plane class configuration mode.  The class-default class map is always at the end of the class map list for a policy map.
<b>Step 4</b>	<b>police</b> [ <b>pps</b> ] { <i>pps-value</i> }	Specifies the rate limit in terms of packets per second ( PPS ). The PPS range is 0 - 20,000. The default PPS is 0.
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> switch(config-pmap-c)# exit switch(config-pmap)#	Exits policy map class configuration mode.
<b>Step 6</b>	<b>exit</b>  <b>Example:</b> switch(config-pmap)# exit switch(config)#	Exits policy map configuration mode.

	Command or Action	Purpose
<b>Step 7</b>	<b>show policy-map type control-plane [expand] [name class-map-name]</b>  <b>Example:</b> <pre>switch(config)# show policy-map type control-plane</pre>	(Optional) Displays the control plane policy map configuration.
<b>Step 8</b>	<b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration.

## Configuring the Control Plane Service Policy

### Before You Begin

Configure a control plane policy map.

### SUMMARY STEPS

1. **configure terminal**
2. **control-plane**
3. **[no] service-policy input policy-map-name**
4. **exit**
5. (Optional) **show running-config copp [all]**
6. (Optional) **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config) #</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>control-plane</b>  <b>Example:</b> <pre>switch(config) # control-plane switch(config-cp) #</pre>	Enters control plane configuration mode.

	Command or Action	Purpose
Step 3	<p>[no] <b>service-policy input</b> <i>policy-map-name</i></p> <p><b>Example:</b>  <pre>switch(config-cp)# service-policy input PolicyMapA</pre></p>	<p>Specifies a policy map for the input traffic. Repeat this step if you have more than one policy map.</p> <p>Use the <b>no service-policy input</b> <i>policy-map-name</i> command to remove the policy from the control plane.</p>
Step 4	<p><b>exit</b></p> <p><b>Example:</b>  <pre>switch(config-cp)# exit switch(config)#</pre></p>	Exits control plane configuration mode.
Step 5	<p><b>show running-config copp [all]</b></p> <p><b>Example:</b>  <pre>switch(config)# show running-config copp</pre></p>	<p>(Optional)  Displays the CoPP configuration.</p>
Step 6	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b>  <pre>switch(config) # copy running-config-startup-config switch(config) #</pre></p>	<p>(Optional)  Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.</p>

## CoPP Show Commands

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

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

Command	Purpose
<code>show running-config aclmgr [all]</code>	Displays the user-configured access control lists (ACLs) in the running configuration. The <b>all</b> 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 <b>all</b> option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

## Displaying the CoPP Configuration Status

### SUMMARY STEPS

1. `show copp status`

### DETAILED STEPS

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

## Monitoring CoPP

### SUMMARY STEPS

1. `show policy-map interface control-plane`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>show policy-map interface control-plane</b>  <b>Example:</b> <pre>switch# show policy-map interface control-plane</pre>	Displays packet-level statistics for all classes that are part of the applied CoPP policy.  Statistics are specified in terms of OutPackets (packets admitted to the control plane) and DropPackets (packets dropped because of rate limiting).

## Clearing the CoPP Statistics

## SUMMARY STEPS

1. (Optional) **show policy-map interface control-plane**
2. **clear copp statistics**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>show policy-map interface control-plane</b>  <b>Example:</b> <pre>switch# show policy-map interface control-plane</pre>	(Optional) Displays the currently applied CoPP policy and per-class statistics.
Step 2	<b>clear copp statistics</b>  <b>Example:</b> <pre>switch# clear copp statistics</pre>	Clears the CoPP statistics.

## CoPP Configuration Examples

### Creating an IP ACL Based on a New Dynamic Class

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

### Creating a CoPP Class and Associating an ACL

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

**Adding a Class to the CoPP Policy**

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

**Modifying 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>
```

**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
```

**Removing a Class from a 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
```

**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-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-routingprotol
  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

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-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-dhcpreg
class-map type control-plane match-any copp-s-dhcpresp
  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
class-map type control-plane match-any copp-s-glean
class-map type control-plane match-any copp-s-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-routingProto1
  match access-group name copp-system-acl-routingproto1
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-snmpp
  match access-group name copp-system-acl-snmpp

```

```
class-map type control-plane match-any copp-ssh
  match access-group name copp-system-acl-ssh
class-map type control-plane match-any copp-stftp
  match access-group name copp-system-acl-stftp
class-map type control-plane match-any copp-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-default
    police pps 400
  class copp-s-l2switched
    police pps 200
  class copp-s-ping
    police pps 100
  class copp-telnet
    police pps 500
  class copp-ssh
    police pps 500
  class copp-sntp
    police pps 500
  class copp-ntp
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-selfIp
    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 1000
  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-icmp
    police pps 200
  class copp-s-bpdu
    police pps 12000
  class copp-tacacsradius
    police pps 400
  class copp-stftp
    police pps 400
```

## 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%
```

## Additional References for CoPP

This section provides additional information related to implementing CoPP.

**Related Documents**

<b>Related Topic</b>	<b>Document Title</b>
Licensing	<i>Cisco NX-OS Licensing Guide</i>
Command reference	<i>Cisco Nexus 3000 Series Command Reference</i>

## Feature History for CoPP

*Table 18: Feature History for CoPP*

<b>Feature Name</b>	<b>Feature Information</b>
CoPP	Introduced in 5.0(3)U2(2)



## INDEX

### A

- AAA [3, 7, 8, 10, 11, 12, 17, 22](#)
  - accounting [7](#)
  - authentication [7](#)
  - benefits [8](#)
  - configuring console login [12](#)
  - default settings [22](#)
  - description [3](#)
  - enabling MSCHAP authentication [17](#)
  - example configuration [22](#)
  - guidelines [12](#)
  - limitations [12](#)
  - prerequisites [11](#)
  - user login process [10](#)
  - verifying configurations [22](#)
- AAA accounting [18](#)
  - configuring default methods [18](#)
- AAA accounting logs [21](#)
  - clearing [21](#)
  - displaying [21](#)
- AAA authorization [56](#)
  - configuring on TACACS+ servers [56](#)
- AAA logins [15](#)
  - enabling authentication failure messages [15](#)
- AAA protocols [7](#)
  - RADIUS [7](#)
  - TACACS+ [7](#)
- AAA server groups [9](#)
  - description [9](#)
- AAA servers [18, 21](#)
  - specifying SNMPv3 parameters [18, 21](#)
  - specifying user roles [21](#)
  - specifying user roles in VSAs [18](#)
- AAA services [8, 9](#)
  - configuration options [9](#)
  - remote [8](#)
- accounting [7](#)
  - description [7](#)
- ACL TCAM regions [99, 101](#)
  - configuring [99](#)
  - reverting to default sizes [101](#)

- ACLs [86, 95](#)
  - identifying traffic by protocols [86](#)
  - VLAN [95](#)
- authentication [7, 9, 10](#)
  - description [7](#)
  - local [7](#)
  - methods [9](#)
  - remote [7](#)
  - user login [10](#)
- authorization [10, 59](#)
  - user login [10](#)
  - verifying commands [59](#)

### B

- BGP [142](#)
  - using with Unicast RPF [142](#)

### C

- changed information [1](#)
  - description [1](#)
- Cisco [20, 27](#)
  - vendor ID [20, 27](#)
- cisco-av-pair [18, 21](#)
  - specifying AAA user parameters [18, 21](#)
- class maps [155, 157](#)
  - configuring for CoPP [157](#)
  - CoPP [155](#)
- commands [59](#)
  - disabling authorization verification [59](#)
  - enabling authorization verification [59](#)
- configuration example [164](#)
- configuration limitations [156](#)
  - CoPP [156](#)
- configuration status [162](#)
  - CoPP [162](#)
- control plane class maps [161](#)
  - verifying the configuration [161](#)

- control plane policy maps [161](#)
    - verifying the configuration [161](#)
  - control plane protection [151, 152](#)
    - classification [151](#)
    - description [151](#)
    - packet types [151](#)
    - rate controlling mechanisms [152](#)
  - control plane service policy, configuring [160](#)
    - CoPP [160](#)
  - CoPP [149, 152, 155, 156, 157, 158, 160, 161, 162](#)
    - class maps [155](#)
    - configuration limitations [156](#)
    - configuration status [162](#)
    - configuring class maps [157](#)
    - configuring policy maps [158](#)
    - control plane service policy, configuring [160](#)
    - default policy [152](#)
    - description [149](#)
    - guidelines [156](#)
    - licensing [156](#)
    - limitations [156](#)
    - monitoring [162](#)
    - policy templates [152](#)
    - restrictions for management interfaces [156](#)
    - verifying the configuration [161](#)
  - CoPP policy [153](#)
    - layer 2 [153](#)
  - CoPP policy maps [158](#)
    - configuring [158](#)
- ## D
- DAI [127, 128](#)
    - default settings [128](#)
    - guidelines [127](#)
    - limitations [127](#)
  - default CoPP policy [152](#)
  - default settings [22, 128](#)
    - AAA [22](#)
    - DAI [128](#)
  - denial-of-service attacks [143](#)
    - IP address spoofing, mitigating [143](#)
  - DHCP binding database, See [DHCP snooping binding database](#)
  - DHCP relay agent [110, 117, 118](#)
    - enabling or disabling [117](#)
    - enabling or disabling VRF support [118](#)
    - VRF support [110](#)
  - DHCP relay binding database [110](#)
    - description [110](#)
  - DHCP snooping [107, 109, 110, 111](#)
    - binding database [109](#)
    - default settings [111](#)
  - DHCP snooping (*continued*)
    - description [107](#)
    - guidelines [110](#)
    - limitations [110](#)
    - overview [107](#)
  - DHCP snooping binding database [109](#)
    - See also [DHCP snooping binding database](#)
    - described [109](#)
    - description [109](#)
    - entries [109](#)
      - See also [DHCP snooping binding database](#)
  - DoS attacks [143](#)
    - Unicast RPF, deploying [143](#)
  - dynamic ARP inspection [123, 124, 125, 126](#)
    - ARP cache poisoning [124](#)
    - ARP requests [123](#)
    - ARP spoofing attack [124](#)
    - DHCP snooping binding database [124](#)
    - function of [124](#)
    - interface trust states [125](#)
    - logging of dropped packets [126](#)
    - network security issues and interface trust states [125](#)
  - Dynamic Host Configuration Protocol snooping, See [DHCP snooping](#)
- ## E
- examples [22](#)
    - AAA configurations [22](#)
- ## F
- feature history [168](#)
    - CoPP [168](#)
- ## G
- guidelines [110, 127, 156](#)
    - CoPP [156](#)
    - DAI [127](#)
    - DHCP snooping [110](#)
- ## I
- IDs [20, 27](#)
    - Cisco vendor ID [20, 27](#)
  - IP ACLs [5](#)
    - description [5](#)

**L**

- layer 2 [153](#)
  - CoPP policy [153](#)
- licensing [143, 156](#)
  - CoPP [156](#)
  - Unicast RPF [143](#)
- limitations [110, 127, 156](#)
  - CoPP [156](#)
  - DAI [127](#)
  - DHCP snooping [110](#)

**M**

- management interfaces [156](#)
  - CoPP restrictions [156](#)
- monitoring [39, 162](#)
  - CoPP [162](#)
  - RADIUS servers [39](#)
- MSCHAP [17](#)
  - enabling authentication [17](#)

**N**

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

**P**

- policy templates [152](#)
  - description [152](#)
- preshared keys [46](#)
  - TACACS+ [46](#)
- privilege level support for TACACS+ authorization [60](#)
  - configuring [60](#)
- privilege roles [62](#)
  - permitting or denying commands for [62](#)

**R**

- RADIUS [4, 25, 26, 28, 35, 43](#)
  - configuring servers [28](#)
  - configuring timeout intervals [35](#)
  - configuring transmission retry counts [35](#)
  - default settings [43](#)
  - description [4](#)
  - example configurations [43](#)
  - network environments [25](#)
  - operations [26](#)

RADIUS (*continued*)

- prerequisites [28](#)
- statistics, displaying [43](#)
- RADIUS server groups [34](#)
  - global source interfaces [34](#)
- RADIUS server preshared keys [31](#)
- RADIUS servers [36, 40, 41, 42, 43](#)
  - configuring timeout interval [36](#)
  - configuring transmission retry count [36](#)
  - deleting hosts [40](#)
  - displaying statistics [42](#)
  - example configurations [43](#)
  - manually monitoring [41](#)
- RADIUS, global preshared keys [30](#)
- RADIUS, periodic server monitoring [39](#)
- RADIUS, server hosts [29](#)
  - configuring [29](#)

**S**

- sample configuration [164](#)
- server groups [9](#)
- SNMPv3 [18, 21](#)
  - specifying AAA parameters [18](#)
  - specifying parameters for AAA servers [21](#)
- source interfaces [34, 54](#)
  - RADIUS server groups [34](#)
  - TACACS+ server groups [54](#)
- SSH [4](#)
  - description [4](#)
- statistics [69](#)
  - TACACS+ [69](#)

**T**

- TACACS+ [4, 45, 46, 47, 48, 59, 63, 69, 70](#)
  - advantages over RADIUS [45](#)
  - configuring [48](#)
  - configuring global timeout interval [63](#)
  - description [4, 45](#)
  - displaying statistics [69](#)
  - example configurations [70](#)
  - field descriptions [70](#)
  - global preshared keys [46](#)
  - limitations [48](#)
  - prerequisites [47](#)
  - preshared key [46](#)
  - user login operation [46](#)
  - verifying command authorization [59](#)
  - verifying configuration [69](#)

TACACS+ command authorization [57, 59](#)  
   configuring [57](#)  
   testing [59](#)

TACACS+ server groups [54](#)  
   global source interfaces [54](#)

TACACS+ servers [49, 64, 65, 68, 69, 70](#)  
   configuring hosts [49](#)  
   configuring TCP ports [65](#)  
   configuring timeout interval [64](#)  
   displaying statistics [69](#)  
   field descriptions [70](#)  
   manually monitoring [68](#)  
   verifying configuration [69](#)

TCAMs [99, 101](#)  
   configuring [99](#)  
   reverting to default sizes [101](#)

TCP ports [65](#)  
   TACACS+ servers [65](#)

Telnet [4](#)  
   description [4](#)

## U

Unicast RPF [141, 142, 143, 144, 146, 147](#)  
   BGP attributes [142](#)  
   BOOTP and [143](#)  
   default settings [144](#)  
   deploying [143](#)  
   description [141](#)

Unicast RPF (*continued*)  
   DHCP and [143](#)  
   example configurations [146](#)  
   FIB [141](#)  
   guidelines [143](#)  
   implementation [142](#)  
   licensing [143](#)  
   limitations [143](#)  
   loose mode [144](#)  
   statistics [143](#)  
   strict mode [144](#)  
   tunneling and [143](#)  
   verifying configuration [147](#)

user login [10](#)  
   authentication process [10](#)  
   authorization process [10](#)

user roles [18, 21](#)  
   specifying on AAA servers [18, 21](#)

## V

vendor-specific attributes [20](#)

VLAN ACLs [95](#)  
   information about [95](#)

VSA s [20](#)  
   format [20](#)  
   protocol options [20](#)  
   support description [20](#)