Cisco Nexus 3000 Series NX-OS Security Command Reference

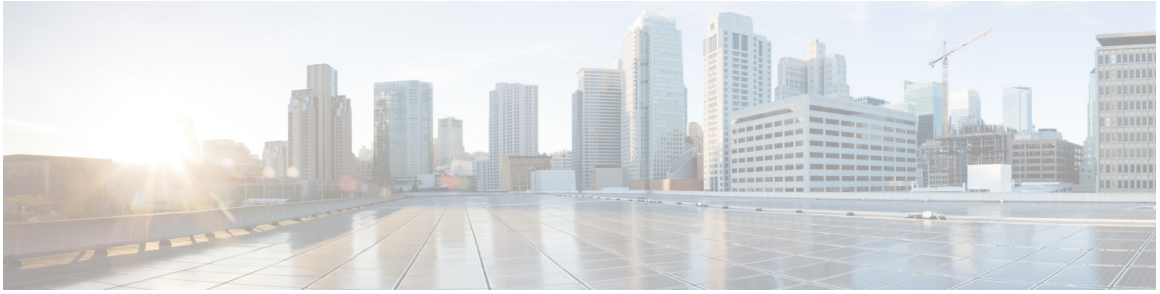
First Published: April 2011
Last Modified: July 2016

Cisco Systems, Inc.
www.cisco.com

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

Text Part Number: OL-26756-03

Cisco Nexus 3000 Series NX-OS Security Command Reference



Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 3000 Series NX-OS Security Command Reference*. It also provides information on how to obtain related documentation.

This preface includes the following sections:

Audience

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

Document Conventions

Command descriptions use these conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use these conventions:

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

This document uses the following conventions:

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

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

Related Documentation

Documentation for the Cisco Nexus 3000 Series Switch is available at the following URL:

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

The documentation set is divided into the following categories:

Release Notes

The release notes are available at the follwing URL:

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

Command References

The command references are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/prod_command_reference_list.html

Technical References

The technical references are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/prod_technical_reference_list.html

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

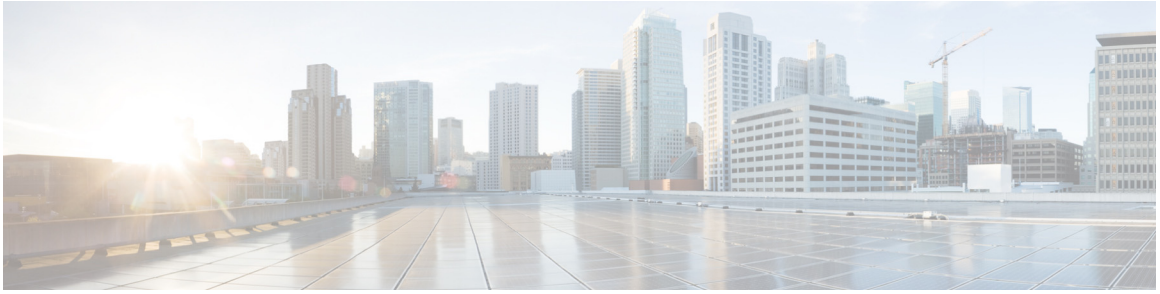
Error and System Messages

The system message reference guide is available at the following URL:

http://www.cisco.com/en/US/products/ps11541/products_system_message_guides_list.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus3k-docfeedback@cisco.com. We appreciate your feedback.



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 Command Reference*. The latest version of this document is available at the following Cisco website:

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

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

http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html

Table 1 summarizes the new and changed features, and tells you where they are documented.

Table 1 New and Changed Information

Feature	Description	Changed in Release	Where Documented
Priortize PACL over SUP TCAM for DHCP	This feature was introduced. Added the **hardware profile pacl priority toggle** command.	6.0(2)U6(7)	hardware profile pacl priority toggle
Telnet	The error message displayed when the telnet service is not detected has changed from “telnet service not enabled” to “Telnet service is disabled.”	7.0(3)I2(1)	show telnet server
TCAM	The output has changed.	7.0(3)I2(1)	show hardware profile tcam region
TCAM	This command is being deprecated in the 7.0(3)I2(1) release.	7.0(3)I2(1)	show platform afm info tcam
Consistency Checker	Command to trigger consistency checkers on RACLS added.	6.0(2)U2(1)	show consistency-checker racl module
ACL Logging	This feature allows you to monitor flows that affect specific access control lists (ACLs)	6.0(2)U2(1)	clear logging ip access-list cache logging level acllog show logging ip access-list cache show logging ip access-list status show logging level acllog show running-config acllog show startup-config acllog

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release	Where Documented
IPv6 DHCP Relay Agent	You can enable the IPv6 DHCP Relay Agent and view its configuration by using these command.	6.0(2)U1(2)	ipv6 dhcp relay ipv6 dhcp relay source-interface show ipv6 dhcp relay clear ipv6 dhcp relay statistics
AAA accounting log	You can enable logging of all commands (including show comands). The **show accounting log** command includes show commands in the command output.	5.0(3)U5(1e)	terminal log-all show accounting log
Syslog Thresholds for System Resources	This feature was introduced.	5.0(3)U3(2)	hardware profile tcam syslog-threshold
DHCP Relay	Added support for Option 82 information to be in encoded string format.	5.0(3)U3(2)	ip dhcp relay information option
IPv6 Support	This feature was introduced. Updated the **hardware profile tcam region** command.	5.0(3)U3(1)	hardware profile tcam region ipv6 access-list ipv6 address ipv6 dhcp relay source-interface ipv6 verify unicast source reachable-via
Address Resolution Protocol (ARP) ACLs for Control plane policing (CoPP)	The following commands were added to include support for CoPP ACLs: • **arp access-lists** • **deny (ARP)** • **permit (ARP)** • **show arp access-lists**	5.0(3)U2(2)	arp access-list deny (ARP) permit (ARP) show arp access-lists
Access Control List (ACL) ternary content addressable memory (TCAM) regions	The following commands were introduced to to change the size of ACL ternary content addressable memory (TCAM) regions: • **hardware profile tcam region** • **show hardware profile tcam region**	5.0(3)U2(1)	hardware profile tcam region show consistency-checker racl module
Address Resolution Protocol (ARP) ACLs for Control plane policing (CoPP)	The following commands were updated to include support for CoPP ACLs: • **deny (IPv4)** • **permit (IPv4)**	5.0(3)U2(1)	deny (IPv4) permit (IPv4)

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release	Where Documented
Access control list (ACL)	This feature was introduced. You can configure ACLs for incoming or outgoing traffic, IPv4 and MAC access lists, or VLAN ACLs.	5.0(3)U1(1)	action clear access-list counters deny (IPv4) ip access-group ip access-list ip port access-group mac port access-group match permit (IPv4) permit interface permit vlan remark resequence vlan access-map vlan filter show access-lists show ip access-lists show running-config acllog show startup-config aclmgr show vlan access-list show vlan access-map show vlan filter
ACLs on VTY	This feature was introduced. You can configure an access class to restrict incoming or outgoing traffic on a virtual terminal line (VTY).	5.0(3)U1(1)	access-class ip access-class

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release	Where Documented
Dynamic Host Configuration Protocol (DHCP) Snooping	This feature was introduced. You can configure DHCP snooping on switches and VLANs.	5.0(3)U1(1)	clear ip dhcp snooping binding clear ip dhcp snooping statistics feature dhcp ip dhcp packet strict-validation ip dhcp relay information option ip dhcp snooping information option ip dhcp snooping trust ip dhcp snooping verify mac-address ip dhcp snooping vlan ip source binding show ip dhcp snooping show ip dhcp snooping binding show ip dhcp snooping statistics show running-config dhcp show startup-config dhcp
Dynamic ARP Inspection (DAI)	This feature was introduced. You can configure dynamic Address Resolution Protocol (ARP) inspection (DAI) on a Cisco NX-OS switch.	5.0(3)U1(1)	clear ip arp clear ip arp inspection log clear ip arp inspection statistics vlan ip arp event-history errors ip arp inspection log-buffer ip arp inspection validate ip arp inspection vlan ip arp inspection trust show ip arp show ip arp inspection show ip arp inspection interfaces show ip arp inspection log show ip arp inspection statistics show ip arp inspection vlan show running-config arp show startup-config arp

Table 1 New and Changed Information (continued)

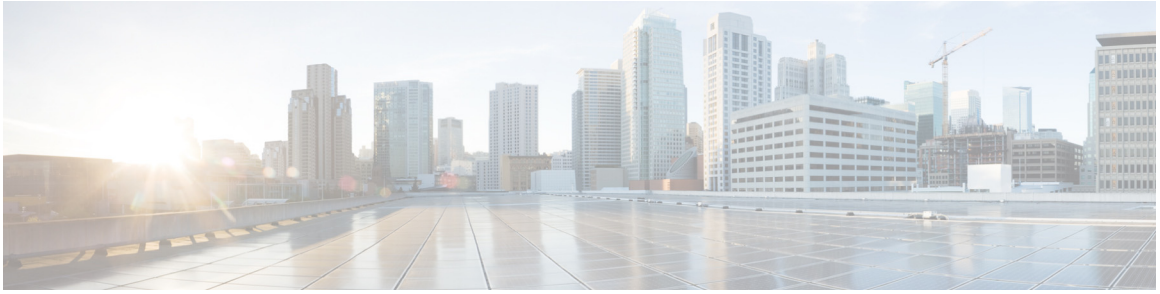
Feature	Description	Changed in Release	Where Documented
Remote Authentication Dial-In User Service (RADIUS)	This feature was introduced. You can configure RADIUS server parameters, the shared secret key, and the number of retransmissions to RADIUS servers.	5.0(3)U1(1)	aaa group server radius deadtime radius-server deadtime radius-server directed-request radius-server host radius-server key radius-server retransmit radius-server timeout server show aaa groups show radius-server show running-config radius
Secure Shell (SSH)	This feature was introduced. You can configure a SSH session using IPv4 or IPv6, or create a SSH server key.	5.0(3)U1(1)	ssh6 ssh ssh key ssh server enable show running-config security show ssh key show ssh server show startup-config security
Telnet	This feature was introduced. You can configure an IPv4 or IPv6 Telnet session and enable a Telnet server.	5.0(3)U1(1)	telnet6 telnet telnet server enable show telnet server

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release	Where Documented
Terminal Access Controller Access-Control System Plus (TACACS+)	This feature was introduced. You can configure the TACACS+ server parameters, enable a secret password for a privilege level, and create user accounts.	5.0(3)U1(1)	deadtime enable enable secret feature privilege feature tacacs+ server tacacs-server deadtime tacacs-server directed-request tacacs-server host tacacs-server key tacacs-server timeout username show privilege show tacacs-server show user-account show users
Authentication, authorization, and accounting (AAA)	This feature was introduced. You can configure AAA authentication methods, authorization methods, accounting methods, Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) authentication, or RADIUS server groups.	5.0(3)U1(1)	aaa accounting default aaa authentication login default aaa authentication login error-enable aaa authentication login mschap enable aaa authorization commands default aaa authorization config-commands default aaa group server radius aaa user default-role show aaa accounting show aaa authentication show aaa authorization show aaa groups show aaa user show access-lists show accounting log show running-config aaa show startup-config aaa

Table 1 New and Changed Information (continued)

Feature	Description	Changed in Release	Where Documented
User roles	This feature was introduced. You can create user roles or user role feature groups.	5.0(3)U1(1)	description (user role) feature (user role feature group) hardware profile tcam syslog-threshold permit vsan role feature-group name role name rule vlan policy deny vsan policy deny show role show role feature show role feature-group show user-account show users
Virtual forwarding and routing (VRF)	This feature was introduced. You can configure VRF, VRF-lite features, and the IP features for a VRF.	5.0(3)U1(1)	permit vrf vrf policy deny use-vrf
System Management	This feature was introduced.	5.0(3)U1(1)	show logging ip access-list cache
Unicast Routing	This feature was introduced.	5.0(3)U1(1)	ip verify unicast source reachable-via



Security Commands

This chapter describes the Cisco NX-OS security commands available on Cisco Nexus 3000 Series switches.

aaa accounting default

To configure authentication, authorization, and accounting (AAA) methods for accounting, use the **aaa accounting default** command. To revert to the default, use the **no** form of this command.

aaa accounting default {**group** {*group-list*} | **local**}

no aaa accounting default {**group** {*group-list*} | **local**}

Syntax Description

group	Specifies that a server group be used for accounting.
group-list	Space-delimited list that specifies one or more configured RADIUS server groups.
local	Specifies that the local database be used for accounting.

Command Default

The local database is the default.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

The **group** *group-list* method refers to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

If you specify the **group** method, or **local** method and they fail, then the accounting authentication can fail.

Examples

This example shows how to configure any RADIUS server for AAA accounting:

```
switch# configure terminal
switch(config)# aaa accounting default group
switch(config)#
```

Related Commands

Command	Description
aaa group server radius	Configures AAA RADIUS server groups.
radius-server host	Configures RADIUS servers.
show aaa accounting	Displays AAA accounting status information.
tacacs-server host	Configures TACACS+ servers.

aaa authentication login ascii-authentication

To enable ASCII authentication for passwords on a TACACS+ server, use the aaa authentication login ascii-authentication command. To revert to the default, use the no form of this command.

aaa authentication login ascii-authentication

no aaa authentication login ascii-authentication

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

Only the TACACS+ protocol supports this feature.

This command does not require a license.

Examples

This example shows how to enable ASCII authentication for passwords on TACACS+ servers:

```
switch# configure terminal
switch(config)# aaa authentication login ascii-authentication
switch(config)#
```

This example shows how to disable ASCII authentication for passwords on TACACS+ servers:

```
switch# configure terminal
switch(config)# no aaa authentication login ascii-authentication
switch(config)#
```

Related Commands

Command	Description
show aaa authentication login ascii-authentication	Displays the status of the ASCII authentication for passwords.

aaa authentication login chap enable

To enable Challenge Handshake Authentication Protocol (MS-CHAP) authentication at login, use the **aaa authentication login chap enable** command. To revert to the default, use the **no** form of this command.

aaa authentication login chap enable

no aaa authentication login chap enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

You cannot enable both CHAP and MSCHAP or MSCHAP V2 on your Cisco NX-OS device.

This command does not require a license.

Examples

This example shows how to enable CHAP authentication:

```
switch# configure terminal
switch(config)# aaa authentication login chap enable
switch(config)#
```

This example shows how to disable CHAP authentication:

```
switch# configure terminal
switch(config)# no aaa authentication login chap enable
switch(config)#
```

Related Commands

Command	Description
show aaa authentication login chap	Displays the status of CHAP authentication.

aaa authentication login console

To configure authentication, authorization, and accounting (AAA) authentication methods for console logins, use the **aaa authentication login console** command. To revert to the default, use the **no** form of this command.

aaa authentication login console {**group** *group-list*} [**none**] | **local** | **none**}

no aaa authentication login console {**group** *group-list* [**none**] | **local** | **none**}

Syntax Description

group	Specifies to use a server group for authentication.
group-list	Space-separated list of RADIUS or TACACS+ server groups. The list can include the following: • **radius** for all configured RADIUS servers. • **tacacs+** for all configured TACACS+ servers. • Any configured RADIUS or TACACS+ server group name.
none	(Optional) Specifies to use the username for authentication.
local	(Optional) Specifies to use the local database for authentication.

Command Default

The local database

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

The **group radius, group tacacs+**, and **group** *group-list* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** or **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

If you specify the **group** method or **local** method and they fail, then the authentication can fail. If you specify the **none** method alone or after the **group** method, then the authentication always succeeds.

Examples

This example shows how to configure the AAA authentication console login method:

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

This example shows how to revert to the default AAA authentication console login method:

```
switch# configure terminal
switch(config)# no aaa authentication login console group radius
switch(config)#
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays AAA authentication information.
tacacs-server host	Configures TACACS+ servers.

aaa authentication login default

To configure the default authentication, authorization, and accounting (AAA) authentication methods, use the **aaa authentication login default** command. To revert to the default, use the **no** form of this command.

aaa authentication login default {**group** *group-list*} [**none**] | **local** | **none**}

no aaa authentication login default {**group** *group-list*} [**none**] | **local** | **none**}

Syntax Description

group	Specifies that a server group be used for authentication.
group-list	Space-separated list of RADIUS or TACACS+ server groups that can include the following: • **radius** for all configured RADIUS servers. • **tacacs+** for all configured TACACS+ servers. • Any configured RADIUS or TACACS+ server group name.
none	(Optional) Specifies that the username be used for authentication.
local	(Optional) Specifies that the local database be used for authentication.

Command Default

The local database

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

The **group radius, group tacacs+**, and **group** *group-list* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** or **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

If you specify the **group** method or **local** method and they fail, then the authentication fails. If you specify the **none** method alone or after the **group** method, then the authentication always succeeds.

Examples

This example shows how to configure the AAA authentication console login method:

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

This example shows how to revert to the default AAA authentication console login method:

```
switch# configure terminal
switch(config)# no aaa authentication login default group radius
switch(config)#
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays AAA authentication information.
tacacs-server host	Configures TACACS+ servers.

aaa authentication login error-enable

To configure that the authentication, authorization, and accounting (AAA) authentication failure message displays on the console, use the **aaa authentication login error-enable** command. To revert to the default, use the **no** form of this command.

aaa authentication login error-enable

no aaa authentication login error-enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

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

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

Examples

This example shows how to enable the display of AAA authentication failure messages to the console:

```
switch# configure terminal
switch(config)# aaa authentication login error-enable
switch(config)#
```

This example shows how to disable the display of AAA authentication failure messages to the console:

```
switch# configure terminal
switch(config)# no aaa authentication login error-enable
switch(config)#
```

Related Commands

Command	Description
show aaa authentication	Displays the status of the AAA authentication failure message display.

aaa authentication login mschap enable

To enable Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) authentication at login, use the **aaa authentication login mschap enable** command. To revert to the default, use the **no** form of this command.

aaa authentication login mschap enable

no aaa authentication login mschap enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to enable MS-CHAP authentication:

```
switch# configure terminal
switch(config)# aaa authentication login mschap enable
switch(config)#
```

This example shows how to disable MS-CHAP authentication:

```
switch# configure terminal
switch(config)# no aaa authentication login mschap enable
switch(config)#
```

Related Commands

Command	Description
show aaa authentication	Displays the status of MS-CHAP authentication.

aaa authentication login mschapv2 enable

To enable Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAP V2) authentication at login, use the **aaa authentication login mschapv2 enable** command. To revert to the default, use the **no** form of this command.

aaa authentication login mschapv2 enable

no aaa authentication login mschapv2 enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

You cannot enable both MSCHAP V2 and CHAP or MSCHAP on your Cisco NX-OS device. This command does not require a license.

Examples

This example shows how to enable MS-CHAP authentication:

```
switch# configure terminal
switch(config)# aaa authentication login mschapv2 enable
switch(config)#
```

This example shows how to disable MS-CHAP authentication:

```
switch# configure terminal
switch(config)# no aaa authentication login mschapv2 enable
switch(config)#
```

Related Commands

Command	Description
show aaa authentication login mschapv2	Displays the status of MS-CHAP V2 authentication.

aaa authorization commands default

To configure default authentication, authorization, and accounting (AAA) authorization methods for all EXEC commands, use the **aaa authorization commands default** command. To revert to the default, use the **no** form of this command.

aaa authorization commands default [**group** *group-list*] [**local** | **none**]

no aaa authorization commands default [**group** *group-list*] [**local** | **none**]

Syntax Description

group	(Optional) Specifies to use a server group for authorization.
group-list	List of server groups. The list can include the following: • **tacacs+** for all configured TACACS+ servers. • Any configured TACACS+ server group name. The name can be a space-separated list of server groups, and a maximum of 127 characters.
local	(Optional) Specifies to use the local role-based database for authorization.
none	(Optional) Specifies to use no database for authorization.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the TACACS+ feature by using the **feature tacacs+** command.

The **group tacacs+** and **group** *group-list* methods refer to a set of previously defined TACACS+ servers. Use the **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers. Use the **show aaa groups** command to display the server groups on the device.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list. The local method or the none method is used only if all the configured server groups fail to respond and you have configured **local** or **none** as the fallback method.

If you specify the **group** method or **local** method and it fails, then the authorization can fail. If you specify the **none** method alone or after the **group** method, then the authorization always succeeds.

Examples

This example shows how to configure the default AAA authorization methods for EXEC commands:

```
switch# configure terminal
switch(config)# aaa authorization commands default group TacGroup local
switch(config)#
```

This example shows how to revert to the default AAA authorization methods for EXEC commands:

```
switch# configure terminal
switch(config)# no aaa authorization commands default group TacGroup local
switch(config)#
```

Related Commands

Command	Description
aaa authorization config-commands default	Configures default AAA authorization methods for configuration commands.
aaa server group	Configures AAA server groups.
feature tacacs+	Enables the TACACS+ feature.
show aaa authorization	Displays the AAA authorization configuration.
tacacs-server host	Configures a TACACS+ server.

aaa authorization config-commands default

To configure the default authentication, authorization, and accounting (AAA) authorization methods for all configuration commands, use the **aaa authorization config-commands default** command. To revert to the default, use the **no** form of this command.

aaa authorization config-commands default [**group** *group-list*] [**local** | **none**]

no aaa authorization config-commands default [**group** *group-list*] [**local** | **none**]

Syntax Description

group	(Optional) Specifies to use a server group for authorization.
group-list	List of server groups. The list can include the following: • **tacacs+** for all configured TACACS+ servers. • Any configured TACACS+ server group name. The name can be a space-separated list of server groups, and a maximum of 127 characters.
local	(Optional) Specifies to use the local role-based database for authorization.
none	(Optional) Specifies to use no database for authorization.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the TACACS+ feature by using the **feature tacacs+** command.

The **group tacacs+** and **group** *group-list* methods refer to a set of previously defined TACACS+ servers. Use the **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers. Use the **show aaa groups** command to display the server groups on the device.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list. The local method or the none method is used only if all the configured server groups fail to respond and you have configured **local** or **none** as the fallback method.

If you specify the **group** method or **local** method and it fails, then the authorization can fail. If you specify the **none** method alone or after the **group** method, then the authorization always succeeds.

Examples

This example shows how to configure the default AAA authorization methods for configuration commands:

```
switch# configure terminal
switch(config)# aaa authorization config-commands default group TacGroup local
switch(config)#
```

This example shows how to revert to the default AAA authorization methods for configuration commands:

```
switch# configure terminal
switch(config)# no aaa authorization config-commands default group TacGroup local
switch(config)#
```

Related Commands

Command	Description
aaa authorization commands default	Configures default AAA authorization methods for EXEC commands.
aaa server group	Configures AAA server groups.
feature tacacs+	Enables the TACACS+ feature.
show aaa authorization	Displays the AAA authorization configuration.
tacacs-server host	Configures a TACACS+ server.

aaa group server radius

To create a RADIUS server group and enter RADIUS server group configuration mode, use the **aaa group server radius** command. To delete a RADIUS server group, use the **no** form of this command.

aaa group server radius *group-name*

no aaa group server radius *group-name*

Syntax Description

group-name	RADIUS server group name.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to create a RADIUS server group and enter RADIUS server configuration mode:

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)#
```

This example shows how to delete a RADIUS server group:

```
switch# configure terminal
switch(config)# no aaa group server radius RadServer
switch(config)#
```

Related Commands

Command	Description
show aaa groups	Displays server group information.

aaa user default-role

To enable the default role assigned by the authentication, authorization, and accounting (AAA) server administrator for remote authentication, use the **aaa user default-role** command. To disable the default role, use the **no** form of this command.

aaa user default-role

no aaa user default-role

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to enable the default role assigned by the AAA server administrator for remote authentication:

```
switch# configure terminal
switch(config)# aaa user default-role
switch(config)#
```

This example shows how to disable the default role assigned by the AAA server administrator for remote authentication:

```
switch# configure terminal
switch(config)# no aaa user default-role
switch(config)#
```

Related Commands

Command	Description
show aaa user default-role	Displays the status of the default user for remote authentication.
show aaa authentication	Displays AAA authentication information.

access-class

To restrict incoming and outgoing connections between a particular VTY (into a Cisco Nexus 3000 Series switch) and the addresses in an access list, use the **access-class** command. To remove access restrictions, use the **no** form of this command.

access-class *access-list-name* {**in** | **out**}

no access-class *access-list-name* {**in** | **out**}

Syntax Description

access-list-name	Name of the IPv4 ACL class. The name can be a maximum of 64 alphanumeric characters. The name cannot contain a space or quotation mark.
in	Specifies that incoming connections be restricted between a particular Cisco Nexus 3000 Series switch and the addresses in the access list.
out	Specifies that outgoing connections be restricted between a particular Cisco Nexus 3000 Series switch and the addresses in the access list.

Command Default

None

Command Modes

Line configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

When you allow telnet or SSH to a Cisco device, you can secure access to the device by binding an access class to the VTYs.

To display the access lists for a particular terminal line, use the **show line** command.

Examples

This example shows how to configure an access class on a VTY line to restrict inbound packets:

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# access-class ozi2 in
switch(config-line)#
```

This example shows how to remove an access class that restricts inbound packets:

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# no access-class ozi2 in
switch(config-line)#
```

Related Commands

Command	Description
ip access-class	Configures an IPv4 access class.
show access-class	Displays the access classes configured on the switch.
show line	Displays the access lists for a particular terminal line.
show running-config aclmgr	Displays the running configuration of ACLs.
ssh	Starts an SSH session using IPv4.
telnet	Starts a Telnet session using IPv4.

action

To specify what the switch does when a packet matches a **permit** command in a VLAN access control list (VACL), use the **action** command. To remove an **action** command, use the **no** form of this command.

action {**drop forward**}

no action {**drop forward**}

Syntax Description

drop	Specifies that the switch drops the packet.
forward	Specifies that the switch forwards the packet to its destination port.

Command Default

None

Command Modes

VLAN access-map configuration
Switch profile configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U2(1)	Support for this command was introduced in switch profiles.

Usage Guidelines

The **action** command specifies the action that the device takes when a packet matches the conditions in the ACL specified by the **match** command.

Examples

This example shows how to create a VLAN access map named vlan-map-01, assign an IPv4 ACL named ip-acl-01 to the map, specify that the switch forwards packets matching the ACL, and enable statistics for traffic matching the map:

```
switch# configure terminal
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
switch(config-access-map)#
```

This example shows how to create a VLAN access map named vlan-map-03 in a switch profile, assign an IPv4 ACL named ip-acl-03 to the map, and specify that the switch drops packets matching the ACL:

```
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)# vlan access-map vlan-map-03
switch(config-sync-sp-access-map)# match ip address ip-acl-03
switch(config-sync-sp-access-map)# action forward
switch(config-sync-sp-access-map)#
```

Related Commands

Command	Description
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
statistics	Enables statistics for an access control list or VLAN access map.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

arp access-list

To create an Address Resolution Protocol (ARP) access control list (ACL) or to enter ARP access list configuration mode for a specific ARP ACL, use the **arp access-list** command. To remove an ARP ACL, use the **no** form of this command.

arp access-list *access-list-name*

no arp access-list *access-list-name*

Syntax Description

access-list-name	Name of the ARP ACL. The name can be up to 64 alphanumeric, case-sensitive characters. Names cannot contain a space or quotation mark.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U2(1)	This command was introduced.

Usage Guidelines

No ARP ACLs are defined by default.

If the ACL specified does not exist, the switch creates it when you enter this command.

Examples

This example shows how to enter the ARP access list configuration mode for an ARP ACL named copp-arp-acl:

```
switch# configure terminal
switch(config)# arp access-list copp-arp-acl
switch(config-arp-acl)#
```

Related Commands

Command	Description
deny (ARP)	Configures a deny rule in an ARP ACL.
permit (ARP)	Configures a permit rule in an ARP ACL.
show arp access-lists	Displays all ARP ACLs or a specific ARP ACL.

clear access-list counters

To clear the counters for all IPv4 access control lists (ACLs) or a single IPv4 ACL, use the **clear access-list counters** command.

clear access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv4 ACL whose counters the switch clears. The name can be a maximum of 64 alphanumeric characters.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to clear counters for all IPv4 ACLs:

```
switch# clear access-list counters
switch#
```

This example shows how to clear counters for an IPv4 ACL named acl-ipv4-01:

```
switch# clear access-list counters acl-ipv4-01
switch#
```

Related Commands

Command	Description
access-class	Applies an IPv4 ACL to a VTY line.
ip access-group	Applies an IPv4 ACL to an interface.
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.
show ip access-lists	Displays information about one or all IPv4 ACLs.

clear accounting log

To clear the accounting log, use the **clear accounting log** command.

clear accounting log

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to clear the accounting log:

```
switch# clear accounting log
switch#
```

Related Commands

Command	Description
show accounting log	Displays the accounting log contents.

clear ip arp

To clear the Address Resolution Protocol (ARP) table and statistics, use the **clear ip arp** command.

clear ip arp [**vlan** *vlan-id* [**force-delete** | **vrf** {*vrf-name* | **all** | **default** | **management**}]]

Syntax Description

vlan *vlan-id*	(Optional) Clears the ARP information for a specified VLAN. The range is from 1 to 4094, except for the VLANs reserved for internal use.
force-delete	(Optional) Clears the entries from ARP table without refresh.
vrf	(Optional) Specifies the virtual routing and forwarding (VRF) to clear from the ARP table.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the ARP table.
default	Specifies that the default VRF entry be cleared from the ARP table.
management	Specifies that the management VRF entry be cleared from the ARP table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to clear the ARP table statistics:

```
switch# clear ip arp
switch#
```

This example shows how to clear the ARP table statistics for VLAN 10 with the VRF vlan-vrf:

```
switch# clear ip arp vlan 10 vrf vlan-vrf
switch#
```

Related Commands

Command	Description
show ip arp	Displays the ARP configuration status.

clear ip arp inspection log

To clear the Dynamic ARP Inspection (DAI) logging buffer, use the **clear ip arp inspection log** command.

clear ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to clear the DAI logging buffer:

```
switch# clear ip arp inspection log
switch#
```

Related Commands

Command	Description
ip arp inspection log-buffer entries	Configures the DAI logging buffer size.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection log	Displays the DAI log configuration.
show ip arp inspection statistics	Displays the DAI statistics.

clear ip arp inspection statistics vlan

To clear the Dynamic ARP Inspection (DAI) statistics for a specified VLAN, use the **clear ip arp inspection statistics vlan** command.

clear ip arp inspection statistics vlan *vlan-list*

Syntax Description

vlan *vlan-list*	Specifies the VLANs whose DAI statistics this command clears. The *vlan-list* argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges. Valid VLAN IDs are from 1 to 4094, except for the VLANs reserved for the internal switch use.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to clear the DAI statistics for VLAN 2:

```
switch# clear ip arp inspection statistics vlan 2
switch#
```

This example shows how to clear the DAI statistics for VLANs 5 through 12:

```
switch# clear ip arp inspection statistics vlan 5-12
switch#
```

This example shows how to clear the DAI statistics for VLAN 2 and VLANs 5 through 12:

```
switch# clear ip arp inspection statistics vlan 2,5-12
switch#
```

Related Commands

Command	Description
clear ip arp inspection log	Clears the DAI logging buffer.
ip arp inspection log-buffer	Configures the DAI logging buffer size.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection vlan	Displays DAI status for a specified list of VLANs.

clear ip dhcp snooping binding

To clear the Dynamic Host Configuration Protocol (DHCP) snooping binding database, use the **clear ip dhcp snooping binding** command.

clear ip dhcp snooping binding [**vlan** *vlan-id* [**mac** *mac-address* **ip** *ip-address*] [**interface** {**ethernet** *slot/port* | **port-channel** *channel-number*}]]

Syntax Description

vlan *vlan-id*	(Optional) Specifies the VLAN ID of the DHCP snooping binding database entry to be cleared. Valid VLAN IDs are from 1 to 4094, except for the VLANs reserved for the internal switch use.
mac-address *mac-address*	(Optional) Specifies the MAC address of the binding database entry to be cleared. Enter the *mac-address* argument in dotted hexadecimal format.
ip *ip-address*	(Optional) Specifies the IPv4 address of the binding database entry to be cleared. Enter the *ip-address* argument in dotted decimal format.
interface	(Optional) Specifies the Ethernet or EtherChannel interface.
ethernet *slot/port*	(Optional) Specifies the Ethernet interface of the binding database entry to be cleared.
port-channel *channel-number*	(Optional) Specifies the Ethernet port channel of the binding database entry to be cleared.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to clear the DHCP snooping binding database:

```
switch# clear ip dhcp snooping binding
switch#
```

This example shows how to clear a specific entry from the DHCP snooping binding database:

```
switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface
ethernet 2/11
switch#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show ip dhcp snooping binding	Displays IP-MAC address bindings, including the static IP source entries.
show running-config dhcp	Displays DHCP snooping configuration.

clear ip dhcp snooping statistics

To clear the Dynamic Host Configuration Protocol (DHCP) snooping statistics, use the **clear ip dhcp snooping statistics** command.

clear ip dhcp snooping statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to clear the DHCP snooping statistics:

```
switch# clear ip dhcp snooping statistics
switch#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show ip dhcp snooping statistics	Displays DHCP snooping statistics.
show running-config dhcp	Displays DHCP snooping configuration.

clear ipv6 dhcp relay statistics

To clear the Dynamic Host Configuration Protocol (DHCP) relay statistics, use the **clear ipv6 dhcp relay statistics** command.

clear ipv6 dhcp relay statistics [interface *interface* **[server-ip** *ip-address* [**interface** *interface*] **[use-vrf** *vrf-name*]]]

Syntax Description

interface *interface*	(Optional) Specifies the interface for which the DHCPv6 relay statistics are to be cleared.
interface *interface* **server-ip** *ip-address* [**interface** *interface*] [**use-vrf** *vrf-name*]	(Optional) Specifies the IPv6 address of the server for the interface specified for which the DHCPv6 relay statistics are to be cleared. Enter the *ip-address* argument in dotted decimal format. The interface can be also be specified after the server ip address.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)U1(2)	This command was introduced.

Examples

This example shows how to clear the DHCPv6 relay statistics:

```
switch# clear ipv6 dhcp relay statistics
switch#
```

This example shows how to clear the DHCPv6 relay statistics at the server level for a specific interface:

```
switch# clear ipv6 dhcp relay statistics interface ethernet 1/1 server-ip 1:2::2 interface
ethernet 1/1 use-vrf red
switch#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ipv6 dhcp relay	Enables the DHCPv6 relay agent.
show ipv6 dhcp relay	Displays DHCPv6 relay configuration.
show running-config dhcp	Displays DHCP snooping configuration.

clear logging ip access-list cache

To clear the access control list (ACL) cache, use the **clear logging ip access-list cache** command.

clear logging ip access-list cache

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)U2(1)	This command was introduced.

Examples

This example shows how to clear the access control list (ACL) cache:

```
switch# clear logging ip access-list cache
```

Command	Description
show logging ip access-list cache	Displays detailed information about the ACL cache.

copp rate-limit disable

To disable the default packets per second sent to the CPU and allow the maximum possible packet rate to the CPU on each queue, use the **copp rate-limit disable** command. To reset the rate limit of the packets to the default value, use the **no** form of this command.

copp rate-limit disable

no copp rate-limit disable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)U1(2)	This command was introduced.

Usage Guidelines

After you run this command, a warning appears to notify you that the CoPP rate-limit is disabled for all classes. Hence, the CPU is vulnerable to traffic attacks. Run the no copp rate-limit disable command as soon as possible.

Caution Disabling the rate limit on CoPP classes can make the CPU vulnerable to overwhelming traffic.

Examples

This example shows how to disable the rate limit on CoPP classes:

```
switch(config)# copp rate-limit disable
switch(config)#
```

deadtime

To configure the dead-time interval for a RADIUS or TACACS+ server group, use the **deadtime** command. To revert to the default, use the **no** form of this command.

deadtime *minutes*

no deadtime *minutes*

Syntax Description

minutes	Number of minutes for the interval. The range is from 0 to 1440 minutes. Setting the dead-time interval to 0 disables the timer.

Command Default

0 minutes

Command Modes

RADIUS server group configuration
TACACS+ server group configuration

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

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

Examples

This example shows how to set the dead-time interval to 2 minutes for a RADIUS server group:

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)# deadtime 2
switch(config-radius)#
```

This example shows how to set the dead-time interval to 5 minutes for a TACACS+ server group:

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# deadtime 5
switch(config-tacacs+)#
```

This example shows how to revert to the dead-time interval default:

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no deadtime 5
switch(config-tacacs+)#
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature tacacs+	Enables TACACS+.
radius-server host	Configures a RADIUS server.
show radius-server groups	Displays RADIUS server group information.
show tacacs-server groups	Displays TACACS+ server group information.
tacacs-server host	Configures a TACACS+ server.

deny (ARP)

To create an ARP ACL rule that denies ARP traffic that matches its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **deny ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac any**

no *sequence-number*

no deny ip {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac any**

Syntax Description

sequence-number	(Optional) Sequence number of the **deny** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
ip	Introduces the IP address portion of the rule.
any	(Optional) Specifies that any host matches the part of the rule that contains the **any** keyword. You can use the **any** to specify the sender IP address, target IP address, sender MAC address, and target MAC address.
host *sender-IP*	(Optional) Specifies that the rule matches ARP packets only when the sender IP address in the packet matches the value of the *sender-IP* argument. Valid values for the *sender-IP* argument are IPv4 addresses in dotted-decimal format.
sender-IP sender-IP-mask	(Optional) IPv4 address and mask for the set of IPv4 addresses that the sender IP address in the packet can match. The *sender-IP* and *sender-IP-mask* argument must be given in dotted-decimal format. Specifying 255.255.255.255 as the *sender-IP-mask* argument is the equivalent of using the **host** keyword.
mac	Introduces the MAC address portion of the rule.

Command Default

None

Command Modes

ARP ACL configuration mode

Command History

Release	Modification
5.0(3)U2(1)	This command was introduced.

Usage Guidelines

Note As of Cisco NX-OS Release 5.0(3)U2(2), ARP access-list is supported only for Control Plane Policing (CoPP). The **deny** command is ignored for CoPP ARP ACLs.

A newly created ARP ACL contains no rules.

If you do not specify a sequence number, the switch assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

When the switch applies an ARP ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

Examples

This example shows how to enter ARP access list configuration mode for an ARP ACL named copp-arp-acl and add a rule that denies ARP request messages that will filter ARP packets coming from sender 192.0.32.14/24 subnet and associate that with the copp-arp-acl class:

```
switch# configure terminal
switch(config)# arp access-list copp-arp-acl
switch(config-arp-acl)# deny ip 192.0.32.14 255.255.255.0 mac any
switch(config-arp-acl)#
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL.
permit (ARP)	Configures a permit rule in an ARP ACL.
remark	Configures a remark in an ACL.
show arp access-list	Displays all ARP ACLs or one ARP ACL.

deny (IPv4)

To create an IPv4 access control list (ACL) rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **deny** *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

no deny *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**][**time-range** *time-range-name*]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*] **deny icmp** *source destination* [*icmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**][**time-range** *time-range-name*]

Internet Group Management Protocol

[*sequence-number*] **deny igmp** *source destination* [*igmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**][**time-range** *time-range-name*]

Internet Protocol v4

[*sequence-number*] **deny ip** *source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**][**time-range** *time-range-name*]

Transmission Control Protocol

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**][**time-range** *time-range-name*] [*flags*] [**established**]

User Datagram Protocol

[*sequence-number*] **deny udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**][**time-range** *time-range-name*]

Syntax Description

sequence-number	(Optional) Sequence number of the **deny** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
protocol	Name or number of the protocol of packets that the rule matches. Valid numbers are from 0 to 255. Valid protocol names are the following keywords: • **ahp**—Specifies that the rule applies to authentication header protocol (AHP) traffic only. • **eigrp**—Specifies that the rule applies to Enhanced Interior Gateway Routing Protocol (EIGRP) traffic only. • **esp**—Specifies that the rule applies to IP Encapsulation Security Payload (ESP) traffic only. • **icmp**—Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **igmp**—Specifies that the rule applies to IGMP traffic only. When you use this keyword, the *igmp-type* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **ip**—Specifies that the rule applies to all IPv4 traffic. When you use this keyword, only the other keywords and arguments that apply to all IPv4 protocols are available. They include the following: – **dscp** – **fragments** – **log** – **precedence** – **time-range** • **nos**—Specifies that the rule applies to IP over IP encapsulation (KA9Q/NOS compatible) traffic only. • **ospf**—Specifies that the rule applies to Open Shortest Path First (OSPF) routing protocol traffic only. • **pcp**—Specifies that the rule applies to IP Payload Compression Protocol (IPComp) traffic only. • **pim**—Specifies that the rule applies to IPv4 Protocol Independent Multicast (PIM) traffic only.

	• **tcp**—Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **udp**—Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
source	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see "Source and Destination" in the "Usage Guidelines" section.
destination	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see "Source and Destination" in the "Usage Guidelines" section.
dscp *dscp*	(Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords: • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010. • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) • **af12**—AF class 1, medium drop probability (001100) • **af13**—AF class 1, high drop probability (001110) • **af21**—AF class 2, low drop probability (010010) • **af22**—AF class 2, medium drop probability (010100) • **af23**—AF class 2, high drop probability (010110) • **af31**—AF class 3, low drop probability (011010) • **af32**—AF class 3, medium drop probability (011100) • **af33**—AF class 3, high drop probability (011110) • **af41**—AF class 4, low drop probability (100010) • **af42**—AF class 4, medium drop probability (100100) • **af43**—AF class 4, high drop probability (100110) • **cs1**—Class-selector (CS) 1, precedence 1 (001000) • **cs2**—CS2, precedence 2 (010000) • **cs3**—CS3, precedence 3 (011000) • **cs4**—CS4, precedence 4 (100000) • **cs5**—CS5, precedence 5 (101000) • **cs6**—CS6, precedence 6 (110000) • **cs7**—CS7, precedence 7 (111000) • **default**—Default DSCP value (000000) • **ef**—Expedited Forwarding (101110)

precedence *precedence*	(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword as follows: • 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011. • **critical**—Precedence 5 (101) • **flash**—Precedence 3 (011) • **flash-override**—Precedence 4 (100) • **immediate**—Precedence 2 (010) • **internet**—Precedence 6 (110) • **network**—Precedence 7 (111) • **priority**—Precedence 1 (001) • **routine**—Precedence 0 (000)
fragments	(Optional) Specifies that the rule matches only those packets that are noninitial fragments. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the switch requires to evaluate those options is contained only in initial fragments.
time-range *time-range-name*	**Note** This keyword is not applicable to a deny rule in a switch profile. (Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command.
icmp-message	(Optional; IGMP only) Rule that matches only packets of the specified ICMP message type. This argument can be an integer from 0 to 255 or one of the keywords listed under “ICMP Message Types” in the “Usage Guidelines” section.
igmp-message	(Optional; IGMP only) Rule that matches only packets of the specified IGMP message type. The *igmp-message* argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords: • **dvmrp**—Distance Vector Multicast Routing Protocol • **host-query**—Host query • **host-report**—Host report • **pim**—Protocol Independent Multicast • **trace**—Multicast trace

operator port [*port*]	(Optional; TCP and UDP only) Rule that matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument must be one of the following keywords: • **eq**—Matches only if the port in the packet is equal to the *port* argument. • **gt**—Matches only if the port in the packet is greater than the *port* argument. • **lt**—Matches only if the port in the packet is less than the *port* argument. • **neq**—Matches only if the port in the packet is not equal to the *port* argument. • **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument.
portgroup *portgroup*	(Optional; TCP and UDP only) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. Use the **object-group ip port** command to create and change IP port-group objects.
flags	(Optional; TCP only) Rule that matches only packets that have specific TCP control bit flags set. The value of the *flags* argument must be one or more of the following keywords: • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	(Optional; TCP only) Specifies that the rule matches only packets that belong to an established TCP connection. The switch considers TCP packets with the ACK or RST bits set to belong to an established connection.

Command Default

A newly created IPv4 ACL contains no rules.

If you do not specify a sequence number, the switch assigns the rule a sequence number that is 10 greater than the last rule in the ACL.

Command Modes

IPv4 ACL configuration
IPv4 ACL in switch profile configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U2(1)	Support for this command was introduced in switch profiles. Support to include **any** or the **host** source address was introduced for IPv4 **deny ip** ACLs. Support was added for the following additional protocols: **ahp**, **eigrp**, **esp**, **nos**, **ospf**, **pcp**, **pim**

Usage Guidelines

When the switch applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  ```
  IPv4-address network-wildcard
  ```

  This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# deny tcp 192.168.67.0 0.0.0.255 any
  ```

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  ```
  IPv4-address/prefix-len
  ```

  This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# deny udp 192.168.67.0/24 any
  ```

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  ```
  host IPv4-address
  ```

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

This example shows how to specify the *source* argument with the **host** keyword and the 192.168.67.132 IPv4 address:

```
switch(config-acl)# deny icmp host 192.168.67.132 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

ICMP Message Types

The *icmp-message* argument can be the ICMP message number, which is an integer from 0 to 255. It can also be one of the following keywords:

- **administratively-prohibited**—Administratively prohibited
- **alternate-address**—Alternate address
- **conversion-error**—Datagram conversion
- **dod-host-prohibited**—Host prohibited
- **dod-net-prohibited**—Net prohibited
- **echo**—Echo (ping)
- **echo-reply**—Echo reply
- **general-parameter-problem**—Parameter problem
- **host-isolated**—Host isolated
- **host-precedence-unreachable**—Host unreachable for precedence
- **host-redirect**—Host redirect
- **host-tos-redirect**—Host redirect for ToS
- **host-tos-unreachable**—Host unreachable for ToS
- **host-unknown**—Host unknown
- **host-unreachable**—Host unreachable
- **information-reply**—Information replies
- **information-request**—Information requests
- **mask-reply**—Mask replies
- **mask-request**—Mask requests
- **mobile-redirect**—Mobile host redirect
- **net-redirect**—Network redirect
- **net-tos-redirect**—Net redirect for ToS
- **net-tos-unreachable**—Network unreachable for ToS
- **net-unreachable**—Net unreachable
- **network-unknown**—Network unknown
- **no-room-for-option**—Parameter required but no room
- **option-missing**—Parameter required but not present
- **packet-too-big**—Fragmentation needed and DF set
- **parameter-problem**—All parameter problems

- **port-unreachable**—Port unreachable
- **precedence-unreachable**—Precedence cutoff
- **protocol-unreachable**—Protocol unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—All redirects
- **router-advertisement**—Router discovery advertisements
- **router-solicitation**—Router discovery solicitations
- **source-quench**—Source quenches
- **source-route-failed**—Source route failed
- **time-exceeded**—All time-exceeded messages
- **timestamp-reply**—Time-stamp replies
- **timestamp-request**—Time-stamp requests
- **traceroute**—Traceroute
- **ttl-exceeded**—TTL exceeded
- **unreachable**—All unreachables

TCP Port Names

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

- **bgp**—Border Gateway Protocol (179)
- **chargen**—Character generator (19)
- **cmd**—Remote commands (rcmd, 514)
- **daytime**—Daytime (13)
- **discard**—Discard (9)
- **domain**—Domain Name Service (53)
- **drip**—Dynamic Routing Information Protocol (3949)
- **echo**—Echo (7)
- **exec**—EXEC (rsh, 512)
- **finger**—Finger (79)
- **ftp**—File Transfer Protocol (21)
- **ftp-data**—FTP data connections (2)
- **gopher**—Gopher (7)
- **hostname**—NIC hostname server (11)
- **ident**—Ident Protocol (113)
- **irc**—Internet Relay Chat (194)
- **klogin**—Kerberos login (543)
- **kshell**—Kerberos shell (544)
- **login**—Login (rlogin, 513)

- **lpd**—Printer service (515)
- **nntp**—Network News Transport Protocol (119)
- **pim-auto-rp**—PIM Auto-RP (496)
- **pop2**—Post Office Protocol v2 (19)
- **pop3**—Post Office Protocol v3 (11)
- **smtp**—Simple Mail Transport Protocol (25)
- **sunrpc**—Sun Remote Procedure Call (111)
- **tacacs**—TAC Access Control System (49)
- **talk**—Talk (517)
- **telnet**—Telnet (23)
- **time**—Time (37)
- **uucp**—Unix-to-Unix Copy Program (54)
- **whois**—WHOIS/NICNAME (43)
- **www**—World Wide Web (HTTP, 8)

UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

- **biff**—Biff (mail notification, comsat, 512)
- **bootpc**—Bootstrap Protocol (BOOTP) client (68)
- **bootps**—Bootstrap Protocol (BOOTP) server (67)
- **discard**—Discard (9)
- **dnsix**—DNSIX security protocol auditing (195)
- **domain**—Domain Name Service (DNS, 53)
- **echo**—Echo (7)
- **isakmp**—Internet Security Association and Key Management Protocol (5)
- **mobile-ip**—Mobile IP registration (434)
- **nameserver**—IEN116 name service (obsolete, 42)
- **netbios-dgm**—NetBIOS datagram service (138)
- **netbios-ns**—NetBIOS name service (137)
- **netbios-ss**—NetBIOS session service (139)
- **non500-isakmp**—Internet Security Association and Key Management Protocol (45)
- **ntp**—Network Time Protocol (123)
- **pim-auto-rp**—PIM Auto-RP (496)
- **rip**—Routing Information Protocol (router, in.routed, 52)
- **snmp**—Simple Network Management Protocol (161)
- **snmptrap**—SNMP Traps (162)
- **sunrpc**—Sun Remote Procedure Call (111)

- **syslog**—System Logger (514)
- **tacacs**—TAC Access Control System (49)
- **talk**—Talk (517)
- **tftp**—Trivial File Transfer Protocol (69)
- **time**—Time (37)
- **who**—Who service (rwho, 513)
- **xdmcp**—X Display Manager Control Protocol (177)

Examples

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules that deny all TCP and UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network and a final rule that permits all other IPv4 traffic:

```
switch# configure terminal
switch(config)# ip access-list acl-lab-01
switch(config-acl)# deny tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny udp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny tcp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# deny udp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit ip any any
switch(config-acl)#
```

This example shows how to configure an IPv4 ACL named sp-acl with rules that deny all AHP and OSPF traffic from the 10.20.0.0 and 192.168.36.0 networks to the 10.172.0.0 network and a final rule that permits all other IPv4 traffic in a switch profile:

```
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)# ip access-list sp-acl
switch(config-sync-sp-acl)# deny ahp 10.20.0.0/16 10.172.0.0/16
switch(config-sync-sp-acl)# deny ospf 10.20.0.0/16 10.172.0.0/16
switch(config-sync-sp-acl)# deny ahp 192.168.36.0/16 10.172.0.0/16
switch(config-sync-sp-acl)# deny ospf 192.168.36.0/16 10.172.0.0/16
switch(config-sync-sp-acl)# permit ip any any
switch(config-sync-sp-acl)#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
remark	Configures a remark in an IPv4 ACL.
show ip access-list	Displays all IPv4 ACLs or one IPv4 ACL.
show switch-profile	Displays information about the switch profile and the configuration revision.
switch-profile	Creates and configures a switch profile.

description (user role)

To configure a description for a user role, use the **description** command. To revert to the default, use the **no** form of this command.

description *text*

no description

Syntax Description

text	Text string that describes the user role. The maximum length is 128 alphanumeric characters.

Command Default

None

Command Modes

User role configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

You can include blank spaces in the user role description text.

Examples

This example shows how to configure the description for a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# description User role for my user account.
switch(config-role)#
```

This example shows how to remove the description from a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# no description
switch(config-role)#
```

Related Commands

Command	Description
show role	Displays information about the user role configuration.

enable

To enable a user to move to a higher privilege level after being prompted for a secret password, use the **enable** command.

enable *level*

Syntax Description

level	Privilege level to which the user must log in. The only available level is 15.

Command Default

Privilege level 15

Command Modes

EXEC configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the cumulative privilege of roles for command authorization on TACACS+ servers using the **feature privilege** command.

Examples

This example shows how to enable the user to move to a higher privilege level after being prompted for a secret password:

```
switch# enable 15
switch#
```

Related Commands

Command	Description
enable secret	Enables a secret password for a specific privilege level.
feature privilege	Enables the cumulative privilege of roles for command authorization on TACACS+ servers.
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.
username	Enables a user to use privilege levels for authorization.

enable secret

To enable a secret password for a specific privilege level, use the **enable secret** command. To disable the password, use the **no** form of this command.

enable secret [**0** | **5**] **password** [**all** | **priv-lvl** *priv-level*]

no enable secret [**0** | **5**] **password** [**all** | **priv-lvl** *priv-level*]

Syntax Description

0	(Optional) Specifies that the password is in clear text.
5	(Optional) Specifies that the password is in encrypted format.
password	Password for user privilege escalation. It contains up to 64 alphanumeric, case-sensitive characters.
all	(Optional) Adds or removes all privilege level secrets.
priv-lvl *priv-level*	(Optional) Specifies the privilege level to which the secret belongs. The range is from 1 to 15.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the cumulative privilege of roles for command authorization on TACACS+ servers using the **feature privilege** command.

Examples

This example shows how to enable a secret password for a specific privilege level:

```
switch# configure terminal
switch(config)# feature privilege
switch(config)# enable secret 5 def456 priv-lvl 15
switch(config)# username user2 priv-lvl 15
switch(config)#
```

Related Commands

Command	Description
enable	Enables the user to move to a higher privilege level after being prompted for a secret password.
feature privilege	Enables the cumulative privilege of roles for command authorization on TACACS+ servers.

Command	Description
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.
username	Enables a user to use privilege levels for authorization.

feature (user role feature group)

To configure a feature in a user role feature group, use the **feature** command. To delete a feature in a user role feature group, use the **no** form of this command.

feature *feature-name*

no feature *feature-name*

Syntax Description

feature-name	Switch feature name as listed in the **show role feature** command output.

Command Default

None

Command Modes

User role feature group configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

Use the **show role** feature command to list the valid feature names to use in this command.

Examples

This example shows how to add features to a user role feature group:

```
switch# configure terminal
switch(config)# role feature-group name SecGroup
switch(config-role-featuregrp)# feature aaa
switch(config-role-featuregrp)# feature radius
switch(config-role-featuregrp)# feature tacacs
switch(config-role-featuregrp)#
```

This example shows how to remove a feature from a user role feature group:

```
switch# configure terminal
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)# no feature callhome
switch(config-role-featuregrp)#
```

Related Commands

Command	Description
role feature-group name	Creates or configures a user role feature group.
show role feature-group	Displays the user role feature groups.

feature dhcp

To enable the Dynamic Host Configuration Protocol (DHCP) snooping feature on the device, use the **feature dhcp** command. To disable the DHCP snooping feature and remove all configuration related to DHCP snooping, use the **no** form of this command.

feature dhcp

no feature dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

The DHCP snooping feature is disabled by default. DHCP snooping can be enabled or disabled on VLANs.

If you have not enabled the DHCP snooping feature, commands related to DCHP snooping are unavailable.

Dynamic ARP inspection depends upon the DHCP snooping feature.

If you disable the DHCP snooping feature, the device discards all configuration related to DHCP snooping configuration, including the following features:

- DHCP snooping
- DHCP relay
- Dynamic ARP Inspection (DAI)

If you want to turn off DHCP snooping and preserve configuration related to DHCP snooping, disable DHCP snooping globally with the **no ip dhcp snooping** command.

Access-control list (ACL) statistics are not supported if the DHCP snooping feature is enabled.

Examples

This example shows how to enable DHCP snooping:

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

This example shows how to disable DHCP snooping:

```
switch# configure terminal
```

```
switch(config)# no feature dhcp
switch(config)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
ip dhcp snooping	Globally enables DHCP snooping on the device.
show running-config dhcp	Displays DHCP snooping configuration.

feature privilege

To enable the cumulative privilege of roles for command authorization on RADIUS and TACACS+ servers, use the **feature privilege** command. To disable the cumulative privilege of roles, use the **no** form of this command.

feature privilege

no feature privilege

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

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

Examples

This example shows how to enable the cumulative privilege of roles:

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

This example shows how to disable the cumulative privilege of roles:

```
switch# configure terminal
switch(config)# no feature privilege
switch(config)#
```

Related Commands

Command	Description
enable	Enables a user to move to a higher privilege level.
enable secret priv-lvl	Enables a secret password for a specific privilege level.
show feature	Displays the features enabled or disabled on the switch.
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.
username	Enables a user to use privilege levels for authorization.

feature tacacs+

To enable TACACS+, use the **feature tacacs+** command. To disable TACACS+, use the **no** form of this command.

feature tacacs+

no feature tacacs+

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

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

Note When you disable TACACS+, the Cisco NX-OS software removes the TACACS+ configuration.

Examples

This example shows how to enable TACACS+:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)#
```

This example shows how to disable TACACS+:

```
switch# configure terminal
switch(config)# no feature tacacs+
switch(config)#
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ information.
show feature	Displays whether or not TACACS+ is enabled on the switch.

hardware profile pacl priority toggle

To change the Priority of the SUP and the PACL region, use the **hardware profile pacl priority toggle** command so that for any conflicting actions PACL region takes priority. Reload the switch for this configuration to take effect.

hardware profile pacl priority toggle

Syntax Description

toggle	Toggles from SUP region to PACL region on priority.

Command Default

None.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)U6(7)	This command was introduced.

Usage Guidelines

Normally entries that are programmed in the SUP region take priority over the entries in PACL region. To toggle from SUP region to PACL region, the command **hardware profile pacl priority toggle** is configured which will take effect after reload just like any other hardware profile commands. During this configuration, when any action on the PACL region has a conflicting action in the SUP region, PACL entry takes priority over the SUP entry.

Examples

Enter the following command in configuration mode as follows:

```
switch(config)# hardware profile pacl priority toggle
```

hardware profile tcam region

To change the size of the access control list (ACL) ternary content addressable memory (TCAM) regions in the hardware, use the **hardware profile tcam region** command. To revert to the default ACL TCAM size, use the **no** form of this command.

hardware profile tcam region {**arpacl** | **e-racl** | **e-vacl** | **ifacl** | **ipv6-e-racl** | **ipv6-qos** | **ipv6-racl** | **ipv6-sup** |**qos** | **qoslbl** | **racl** | **vacl**} *tcam_size*

no hardware profile tcam region {**arpacl** | **e-racl** | **e-vacl** | **ifacl** | **ipv6-e-racl** | **ipv6-qos** | **ipv6-racl** | **ipv6-sup** |**qos** | **qoslbl** | **racl** | **vacl**} *tcam_size*

Syntax Description

arpacl	Configures the size of the Address Resolution Protocol (ARP) ACL (ARPACL) TCAM region.
e-racl	Configures the size of the egress router ACL (ERACL) TCAM region.
e-vacl	Configures the size of the egress VLAN ACL (EVACL) TCAM region.
ifacl	Configures the size of the interface ACL (ifacl) TCAM region.
ipv6-e-racl	Configures the size of the egress router ACL (ERACL) TCAM region for IPv6.
ipv6-qos	Configures the size of the quality of service (QoS) TCAM region for IPv6.
ipv6-racl	Configures the size of the router ACL (ERACL) TCAM region for IPv6.
ipv6-sup	Configures the size of the Supervisor TCAM region for IPv6.
qos	Configures the size of the quality of service (QoS) TCAM region.
qoslbl	Configures the size of the QoS Label (qoslbl) TCAM region.
racl	Configures the size of the router ACL (RACL) TCAM region.
vacl	Configures the size of the VLAN ACL (VACL) TCAM region.
tcam_size	TCAM size. The range is from 0 to 2,14,74,83,647 entries.

Command Default

None

Command Modes

Global configuration mode
Switch profile configuration mode

Command History

Release	Modification
5.0(3)U3(1)	Added the **no** form of this command.
5.0(3)U2(1)	This command was introduced.

Usage Guidelines

When you change the TCAM size, the new TCAM size is saved in the running configuration. To apply the new TCAM size, you must copy the running configuration of the switch to the startup configuration file (**copy running-config startup-config** command) and then reload (**reload** command) the switch.

Note Make sure that you set the VACL and EVACL size to the same value.

Table 1 lists the default TCAM size for each ACL region:

Table 1 Default, Minimum and Maximum Size for ACL TCAM Regions

TCAM Region	Default Size	Minimum	Increment	Max
ARPCL	0	0	128	128
PACL	384	128 or 256[1]	256	1664 combined
VACL	512	0	256	
RACL	512	256	256	
QOS	256	256	256	
RACL_IPV6	0	0	256X2	
QOS_IPV6	0	0	256X2	1024 combined
E-VACL	512	0	256	
E-RACL_IPV6	0	0	256X2	
QOSLBL	256	256	256	1024 combined
SUP_IPV6	256X2	256X2	—	

[1]128 if the ARPACL is disabled and 256 if the ARPACL is enabled.

Note The default size of the ARPACL TCAM is zero. Before you use the ARP ACLs in a Control Plane Policing (CoPP) policy, you must set the size of this TCAM to a nonzero size.

Examples

This example shows how to change the size of the RACL TCAM region:

```
switch# configure terminal
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#

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

This example shows 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# configure terminal
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 =  384
         qos size =  256
       rbacl size =    0
        span size =  128
        racl size =  512
      e-racl size =  512
      e-vacl size =  512
      qoslbl size =  256
      arpacl size =    0
   ipv6-racl size =    0
 ipv6-e-racl size =    0
    ipv6-sup size =  256
    ipv6-qos size =    0

switch(config)#
```

This example shows how to configure the TCAM VLAN ACLs on a switch profile:

```
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)#
```

This example shows how to revert to the default ACL TCAM size:

```
switch (config)# no hardware profile tcam region arpacl 128
To stop using ARPACL tcam, IFACL tcam size needs to be changed. Changing IFACL tcam size
to 384
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

switch(config)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration file.
reload	Reloads the switch.
show hardware profile tcam region	Displays the TCAM sizes that will be applicable on the next reload of the switch.
show running-config	Displays the information for the running configuration.
write erase	Erases the configuration in persistent memory.

hardware profile tcam syslog-threshold

To configure the syslog threshold for the ACL TCAM so that a syslog message is generated when the TCAM capacity reaches the specified percentage, use the **hardware profile tcam syslog-threshold** command. To reset the value to the default, use the **no** form of this command.

hardware profile tcam syslog-threshold *percentage*

no hardware profile tcam syslog-threshold

Syntax Description

percentage	Percentage of the TCAM capacity. The range is from 1 to 100. The default value is 90 percent.

Defaults

The ACL TCAM threshold is 90 percent.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U3(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to set the syslog threshold to 20 percent for the ACL TCAM:

```
switch# configure terminal
switch(config)# hardware profile tcam syslog-threshold 20
switch(config)#
```

Related Commands

Command	Description
copy running-config startup config	Copies the running configuration to the startup configuration file.
show running-config	Displays the information for the running configuration.

interface policy deny

To enter interface policy configuration mode for a user role, use the **interface policy deny** command. To revert to the default interface policy for a user role, use the **no** form of this command.

interface policy deny

no interface policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

All interfaces

Command Modes

User role configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to enter interface policy configuration mode for a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)#
```

This example shows how to revert to the default interface policy for a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# no interface policy deny
switch(config-role)#
```

Related Commands

Command	Description
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

ip access-class

To create or configure an IPv4 access class to restrict incoming or outgoing traffic on a virtual terminal line (VTY), use the **ip access-class** command. To remove the access class, use the **no** form of this command.

ip access-class *access-list-name* {**in** | **out**}

no ip access-class *access-list-name* {**in** | **out**}

Syntax Description

access-list-name	Name of the IPv4 ACL class. The name can be a maximum of 64 characters. The name can contain characters, numbers, hyphens, and underscores. The name cannot contain a space or quotation mark.
in	Specifies that incoming connections be restricted between a particular Cisco Nexus 3000 Series switch and the addresses in the access list.
out	Specifies that outgoing connections be restricted between a particular Cisco Nexus 3000 Series switch and the addresses in the access list.

Command Default

None

Command Modes

Line configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to configure an IP access class on a VTY line to restrict inbound packets:

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# ip access-class VTY_ACCESS in
switch(config-line)#
```

This example shows how to remove an IP access class that restricts inbound packets:

```
switch(config)# line vty
switch(config-line)# no ip access-class VTY_ACCESS in
switch(config-line)#
```

Related Commands

Command	Description
access-class	Configures an access class for VTY.
copy running-config startup-config	Copies the running configuration to the startup configuration file.
show line	Displays the access lists for a particular terminal line.

Command	Description
show running-config aclmgr	Displays the running configuration of ACLs.
show startup-config aclmgr	Displays the startup configuration for ACLs.
ssh	Starts an SSH session using IPv4.
telnet	Starts a Telnet session using IPv4.

ip access-group

To apply an IPv4 access control list (ACL) to a Layer 3 interface as a router ACL, use the **ip access-group** command. To remove an IPv4 ACL from an interface, use the **no** form of this command.

ip access-group *access-list-name* {**in** | **out**}

no ip access-group *access-list-name* {**in** | **out**}

Syntax Description

access-list-name	Name of the IPv4 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
in	Specifies that the ACL applies to inbound traffic.
out	Specifies that the ACL applies to outbound traffic.

Command Default

None

Command Modes

Interface configuration mode
Subinterface configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

By default, no IPv4 ACLs are applied to a Layer 3 routed interface.

You can use the **ip access-group** command to apply an IPv4 ACL as a router ACL to the following interface types:

- VLAN interfaces
- Layer 3 Ethernet interfaces
- Layer 3 Ethernet subinterfaces
- Layer 3 Ethernet port-channel interfaces and subinterfaces
- Loopback interfaces
- Management interfaces

You can also use the **ip access-group** command to apply an IPv4 ACL as a router ACL to the following interface types:

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

However, an ACL applied to a Layer 2 interface with the **ip access-group** command is inactive unless the port mode changes to routed (Layer 3) mode.

If you delete the specified ACL from the device without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

This command does not require a license.

Examples

This example shows how to apply an IPv4 ACL named ip-acl-01 to the Layer 3 Ethernet interface 2/1:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip access-group ip-acl-01 in
switch(config-if)#
```

This example shows how to remove an IPv4 ACL named ip-acl-01 from Ethernet interface 2/1:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip access-group ip-acl-01 in
switch(config-if)# no ip access-group ip-acl-01 in
switch(config-if)#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs.
show ip access-lists	Shows either a specific IPv4 ACL or all IPv4 ACLs.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.

ip access-list

To create an IPv4 access control list (ACL) or to enter IP access list configuration mode for a specific ACL, use the **ip access-list** command. To remove an IPv4 ACL, use the **no** form of this command.

ip access-list *access-list-name*

no ip access-list *access-list-name*

Syntax Description

access-list-name	Name of the IPv4 ACL, which can be up to 64 alphanumeric characters long. The name cannot contain a space or quotation mark.

Command Default

No IPv4 ACLs are defined by default.

Command Modes

Global configuration mode
Switch profile configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U2(1)	Support was added to configure IP features in a switch profile.

Usage Guidelines

Use IPv4 ACLs to filter IPv4 traffic.

When you use the **ip access-list** command, the switch enters IP access list configuration mode, where you can use the IPv4 **deny** and **permit** commands to configure rules for the ACL. If the specified ACL does not exist, the switch creates it when you enter this command.

Use the **ip access-group** command to apply the ACL to an interface.

Every IPv4 ACL has the following implicit rule as its last rule:

```
deny ip any any
```

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

IPv4 ACLs do not include additional implicit rules to enable the neighbor discovery process. The Address Resolution Protocol (ARP), which is the IPv4 equivalent of the IPv6 neighbor discovery process, uses a separate data link layer protocol. By default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Use the **match-local-traffic** option for all inbound and outbound traffic to or from the CPU.

Examples

This example shows how to enter IP access list configuration mode for an IPv4 ACL named ip-acl-01:

```
switch# configure terminal
switch(config)# ip access-list ip-acl-01
switch(config-acl)#
```

This example shows how to enter IP access list configuration mode for an IPv4 ACL named sp-acl in a switch profile:

```
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)# ip access-list sp-acl
switch(config-sync-sp-acl)#
```

Related Commands

Command	Description
access-class	Applies an IPv4 ACL to a VTY line.
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
ip access-group	Applies an IPv4 ACL to an interface.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
show switch-profile	Displays information about the switch profile and the configuration revision.
switch-profile	Creates and configures a switch profile.

ip arp event-history errors

To log Address Resolution Protocol (ARP) debug events into the event history buffer, use the **ip arp event-history errors** command.

ip arp event-history errors size {**disabled** | **large** | **medium** | **small**}

no ip arp event-history errors size {**disabled** | **large** | **medium** | **small**}

Syntax Description

size	Specifies the event history buffer size to configure.
disabled	Specifies that the event history buffer size is disabled.
large	Specifies that the event history buffer size is large.
medium	Specifies that the event history buffer size is medium.
small	Specifies that the event history buffer size is small. This is the default buffer size.

Command Default

By default, the event history buffer is small.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to configure a medium ARP event history buffer:

```
switch# configure terminal
switch(config)# ip arp event-history errors size medium
switch(config)#
```

This example shows how to set the ARP event history buffer to the default:

```
switch# configure terminal
switch(config)# no ip arp event-history errors size medium
switch(config)#
```

Related Commands

Command	Description
show running-config arp all	Displays the ARP configuration, including the default configurations.

ip arp inspection log-buffer

To configure the Dynamic ARP Inspection (DAI) logging buffer size, use the **ip arp inspection log-buffer** command. To reset the DAI logging buffer to its default size, use the **no** form of this command.

ip arp inspection log-buffer entries *number*

no ip arp inspection log-buffer entries *number*

Syntax Description

entries *number*	Specifies the buffer size in a range of 1 to 1024 messages.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

Before you use this command, make sure that you enable Dynamic Host Configuration Protocol (DHCP) snooping on the switch by using the **feature dhcp** command.

By default, the DAI logging buffer size is 32 messages.

Examples

This example shows how to configure the DAI logging buffer size:

```
switch# configure terminal
switch(config)# ip arp inspection log-buffer entries 64
switch(config)#
```

Related Commands

Command	Description
clear ip arp inspection log	Clears the DAI logging buffer.
feature dhcp	Enables DHCP snooping.
show ip arp inspection log	Displays the DAI log configuration.
show running-config dhcp	Displays DHCP snooping configuration, including the DAI configuration.

ip arp inspection validate

To enable additional Dynamic ARP Inspection (DAI) validation, use the **ip arp inspection validate** command. To disable additional DAI, use the **no** form of this command.

ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**]}

ip arp inspection validate {**ip** [**dst-mac**] [**src-mac**]}

ip arp inspection validate {**src-mac** [**dst-mac**] [**ip**]}

no ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**]}

no ip arp inspection validate {**ip** [**dst-mac**] [**src-mac**]}

no ip arp inspection validate {**src-mac** [**dst-mac**] [**ip**]}

Syntax Description

dst-mac	(Optional) Enables validation of the destination MAC address in the Ethernet header against the target MAC address in the ARP body for ARP responses. The device classifies packets with different MAC addresses as invalid and drops them.
ip	(Optional) Enables validation of the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. The device checks the sender IP addresses in all ARP requests and responses and checks the target IP addresses only in ARP responses.
src-mac	(Optional) Enables validation of the source MAC address in the Ethernet header against the sender MAC address in the ARP body for ARP requests and responses. The devices classifies packets with different MAC addresses as invalid and drops them.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

Before you use this command, make sure that you enable Dynamic Host Configuration Protocol (DHCP) snooping on the switch by using the **feature dhcp** command.

You must specify at least one keyword. If you specify more than one keyword, the order is irrelevant.

When you enable source MAC validation, an ARP packet is considered valid only if the sender Ethernet address in the packet body is the same as the source Ethernet address in the ARP frame header. When you enable destination MAC validation, an ARP request frame is considered valid only if the target Ethernet address is the same as the destination Ethernet address in the ARP frame header.

Examples

This example shows how to enable additional DAI validation:

```
switch# configure terminal
switch(config)# ip arp inspection validate src-mac dst-mac ip
switch(config)#
```

This example shows how to disable additional DAI validation:

```
switch# configure terminal
switch(config)# no ip arp inspection validate src-mac dst-mac ip
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables DHCP snooping.
show ip arp inspection	Displays the DAI configuration status.
show running-config dhcp	Displays DHCP snooping configuration, including DAI configuration.

ip arp inspection vlan

To enable Dynamic ARP Inspection (DAI) for a list of VLANs, use the **ip arp inspection vlan** command. To disable DAI for a list of VLANs, use the **no** form of this command.

ip arp inspection vlan *vlan-list* [**logging dhcp-bindings** {**permit** | **all** | **none**}]

no ip arp inspection vlan *vlan-list* [**logging dhcp-bindings** {**permit** | **all** | **none**}]

Syntax Description

vlan-list	VLANs on which DAI is active. The vlan-list argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the "Examples" section). Valid VLAN IDs are from 1 to 4096.
logging	(Optional) Enables DAI logging for the VLANs specified. • **all**—Logs all packets that match Dynamic Host Configuration Protocol (DHCP) bindings • **none**—Does not log DHCP bindings packets (use this option to disable logging) • **permit**—Logs DHCP binding permitted packets
dhcp-bindings	Enables logging based on DHCP binding matches.
permit	Enables logging of packets permitted by a DHCP binding match.
all	Enables logging of all packets.
none	Disables logging.

Command Default

Logging of dropped packets

Command Modes

Global configuration

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

By default, the device logs dropped packets inspected by DAI.

This command does not require a license.

Examples

This example shows how to enable DAI on VLANs 13, 15, and 17 through 23:

```
switch# configure terminal
switch(config)# ip arp inspection vlan 13,15,17-23
switch(config)#
```

Related Commands

Command	Description
ip arp inspection validate	Enables additional DAI validation.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection vlan	Displays DAI status for a specified list of VLANs.
show running-config dhcp	Displays DHCP snooping configuration, including DAI configuration.

ip arp inspection trust

To configure a Layer 2 interface as a trusted ARP interface, use the **ip arp inspection trust** command. To configure a Layer 2 interface as an untrusted ARP interface, use the **no** form of this command.

ip arp inspection trust

no ip arp inspection trust

Syntax Description

This command has no arguments or keywords.

Command Default

By default, all interfaces are untrusted ARP interfaces.

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

You can configure only Layer 2 Ethernet interfaces as trusted ARP interfaces.

This command does not require a license.

Examples

This example shows how to configure a Layer 2 interface as a trusted ARP interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip arp inspection trust
switch(config-if)#
```

Related Commands

Command	Description
show ip arp inspection	Displays the Dynamic ARP Inspection (DAI) configuration status.
show ip arp inspection interface	Displays the trust state and the ARP packet rate for a specified interface.
show running-config dhcp	Displays DHCP snooping configuration, including DAI configuration.

ip dhcp packet strict-validation

To enable the strict validation of Dynamic Host Configuration Protocol (DHCP) packets by the DHCP snooping feature, use the **ip dhcp packet strict-validation** command. To disable the strict validation of DHCP packets, use the **no** form of this command.

ip dhcp packet strict-validation

no ip dhcp packet strict-validation

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

You must enable DHCP snooping before you can use the **ip dhcp packet strict-validation** command.

Strict validation of DHCP packets checks that the DHCP options field in DCHP packets is valid, including the "magic cookie" value in the first four bytes of the options field. When strict validation of DHCP packets is enabled, the device drops DHCP packets that fail validation.

Examples

This example shows how to enable the strict validation of DHCP packets:

```
switch# configure terminal
switch(config)# ip dhcp packet strict-validation
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables DHCP snooping on the switch.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays the current DHCP configuration.

ip dhcp relay information option

To enable the device to insert and remove Option 82 information on DHCP packets forwarded by the relay agent, use the **ip dhcp relay information option** command. To globally disable this feature, use the **no** form of this command.

ip dhcp relay information option

no ip dhcp relay information option

Syntax Description

circuit-id format-type string	Specifies to use the encoded string format instead of the default binary ifindex format for Option 82.

Command Default

By default, Option 82 information insertion and removal is globally disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U3(2)	Added support for Option 82 information to be in encoded string format.

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

The device preserves DHCP snooping configuration when you disable DHCP snooping with the **no ip dhcp snooping** command.

Examples

This example shows how to globally enable DHCP relay information and specify an encoded sting format:

```
switch# configure terminal
switch(config)# ip dhcp relay information option circuit-id format-type string
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp smart realy	Enables DHCP smart relay globally.
show running-config dhcp	Displays DHCP snooping configuration.

ip dhcp smart relay

To enable DHCP smart relay globally, use the **ip dhcp smart relay** command. To globally disable this feature, use the **no** form of this command.

ip dhcp smart relay

no ip dhcp smart relay

Syntax Description

This command has no arguments or keywords.

Command Default

By default, this feature is globally disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

The device preserves DHCP snooping configuration when you disable DHCP snooping with the **no ip dhcp snooping** command.

Examples

This example shows how to globally enable DHCP smart relay:

```
switch# configure terminal
switch(config)# ip dhcp smart relay
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
show ip dhcp relay	Displays IP DHCP smart relay configuration.
show running-config dhcp	Displays DHCP snooping configuration.

ip dhcp snooping

To globally enable Dynamic Host Configuration Protocol (DHCP) snooping on the device, use the **ip dhcp snooping** command. To globally disable DHCP snooping, use the **no** form of this command.

ip dhcp snooping

no ip dhcp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

By default, DHCP snooping is globally disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

The device preserves DHCP snooping configuration when you disable DHCP snooping with the **no ip dhcp snooping** command.

Examples

This example shows how to globally enable DHCP snooping:

```
switch# configure terminal
switch(config)# ip dhcp snooping
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping information option	Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.
ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays DHCP snooping configuration.

ip dhcp snooping information option

To enable the insertion and removal of option-82 information for Dynamic Host Configuration Protocol (DHCP) packets, use the **ip dhcp snooping information option** command. To disable the insertion and removal of option-82 information, use the **no** form of this command.

ip dhcp snooping information option

no ip dhcp snooping information option

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the device does not insert and remove option-82 information.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

Examples

This example shows how to globally enable DHCP snooping:

```
switch# configure terminal
switch(config)# ip dhcp snooping information option
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping	Globally enables DHCP snooping on the device.
ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays DHCP snooping configuration.

ip dhcp snooping trust

To configure an interface as a trusted source of Dynamic Host Configuration Protocol (DHCP) messages, use the **ip dhcp snooping trust** command. To configure an interface as an untrusted source of DHCP messages, use the **no** form of this command.

ip dhcp snooping trust

no ip dhcp snooping trust

Syntax Description

This command has no arguments or keywords.

Command Default

By default, no interface is a trusted source of DHCP messages.

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the DHCP snooping feature (see the **feature dhcp** command).

You can configure DHCP trust on the following types of interfaces:

- Layer 3 Ethernet interfaces and subinterfaces
- Layer 2 Ethernet interfaces
- Private VLAN interfaces

Examples

This example shows how to configure an interface as a trusted source of DHCP messages:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip dhcp snooping trust
switch(config-if)#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping on the device.
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays DHCP snooping configuration.

ip dhcp snooping verify mac-address

To enable Dynamic Host Configuration Protocol (DHCP) snooping for MAC address verification, use the **ip dhcp snooping verify mac-address** command. To disable DHCP snooping MAC address verification, use the **no** form of this command.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

By default, MAC address verification with DHCP snooping is not enabled.

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

If the device receives a packet on an untrusted interface and the source MAC address and the DHCP client hardware address do not match, address verification causes the device to drop the packet.

Examples

This example shows how to enable DHCP snooping for MAC address verification:

```
switch# configure terminal
switch(config)# ip dhcp snooping verify mac-address
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables DHCP snooping on the switch.
show running-config dhcp	Displays the DHCP snooping configuration configuration.

ip dhcp snooping vlan

To enable Dynamic Host Configuration Protocol (DHCP) snooping on one or more VLANs, use the **ip dhcp snooping vlan** command. To disable DHCP snooping on one or more VLANs, use the **no** form of this command.

ip dhcp snooping vlan *vlan-list*

no ip dhcp snooping vlan *vlan-list*

Syntax Description

vlan-list	Range of VLANs on which to enable DHCP snooping. The *vlan-list* argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges. Valid VLAN IDs are from 1 to 4094, except for the VLANs reserved for internal use. Use a hyphen (-) to separate the beginning and ending IDs of a range of VLAN IDs; for example, 70-100. Use a comma (,) to separate individual VLAN IDs and ranges of VLAN IDs; for example, 20,70-100,142.

Command Default

By default, DHCP snooping is not enabled on any VLAN.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

Examples

This example shows how to enable DHCP snooping on VLANs 100, 200, and 250 through 252:

```
switch# configure terminal
switch(config)# ip dhcp snooping vlan 100,200,250-252
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables DHCP snooping on the switch.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays DHCP snooping configuration.

ip port access-group

To apply an IPv4 access control list (ACL) to an interface as a port ACL, use the **ip port access-group** command. To remove an IPv4 ACL from an interface, use the **no** form of this command.

ip port access-group *access-list-name* **in**

no ip port access-group *access-list-name* **in**

Syntax Description

access-list-name	Name of the IPv4 ACL, which can be up to 64 alphanumeric, case-sensitive characters long.
in	Specifies that the ACL applies to inbound traffic.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

By default, no IPv4 ACLs are applied to an interface.

You can use the **ip port access-group** command to apply an IPv4 ACL as a port ACL to the following interface types:

- Layer 2 Ethernet interfaces
- Layer 2 EtherChannel interfaces

You can also apply an IPv4 ACL as a VLAN ACL. For more information, see the **match** command.

The switch applies port ACLs to inbound traffic only. The switch checks inbound packets against the rules in the ACL. If the first matching rule permits the packet, the switch continues to process the packet. If the first matching rule denies the packet, the switch drops the packet and returns an ICMP host-unreachable message.

If you delete the specified ACL from the switch without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

Examples

This example shows how to apply an IPv4 ACL named ip-acl-01 to Ethernet interface 1/2 as a port ACL:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip port access-group ip-acl-01 in
switch(config-if)#
```

This example shows how to remove an IPv4 ACL named ip-acl-01 from Ethernet interface 1/2:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no ip port access-group ip-acl-01 in
switch(config-if)#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs.
show ip access-lists	Shows either a specific IPv4 ACL or all IPv4 ACLs.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.

ip source binding

To create a static IP source entry for a Layer 2 Ethernet interface, use the **ip source binding** command. To disable the static IP source entry, use the **no** form of this command.

ip source binding *IP-address MAC-address* **vlan** *vlan-id* {**interface ethernet** *slot/port* | **port-channel** *channel-no*}

no ip source binding *IP-address MAC-address* **vlan** *vlan-id* {**interface ethernet** *slot/port* | **port-channel** *channel-no*}

Syntax Description

IP-address	IPv4 address to be used on the specified interface. Valid entries are in dotted-decimal format.
MAC-address	MAC address to be used on the specified interface. Valid entries are in dotted-hexadecimal format.
vlan *vlan-id*	Specifies the VLAN associated with the IP source entry.
interface ethernet *slot/port*	Specifies the Layer 2 Ethernet interface associated with the static IP entry. The slot number can be from 1 to 255, and the port number can be from 1 to 128.
port-channel *channel-no*	Specifies the EtherChannel interface. The number cna be from 1 to 4096.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

By default, there are no static IP source entries.

To use this command, you must enable the Dynamic Host Configuration Protocol (DHCP) snooping feature using the **feature dhcp** command.

Examples

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)#
```

Related Commands

Command	Description
feature dhcp	Enables DHCP snooping on the switch.
show ip verify source	Displays IP-to-MAC address bindings.
show interface	Displays interface configuration.
show running-config dhcp	Displays the DHCP snooping configuration information.

ipv6 address

To configure an IPv6 address on an interface, use the **ipv6 address** command. To remove the IPv6 address configuration, use the **no** form of this command.

ipv6 address {ipv6-*address* [**eui64**] [**route-preference** *preference*] [**secondary**] [**tag** *tag-id*]} {**use-link-local-only**}

no ipv6 address {ipv6-*address* [**eui64**] [**route-preference** *preference*] [**secondary**] [**tag** *tag-id*]} {**use-link-local-only**}

Syntax Description

ipv6-address	IPv6 address. The format is A:B::C:D/length. The length range is 1 to 128.
eui64	(Optional) Configures the Extended Unique Identifier (EUI64) for the low-order 64 bits of the address.
route-preference *preference*	(Optional) Sets the route preference for local or direct routes. The range is from 0 to 255.s
secondary	(Optional) Creates a secondary IPv6 address.
tag *tag-id*	(Optional) Configures a route tag value for local or direct routes.
use-link-local-only	Specifies IPv6 on the interface by using only a single link-local.

Defaults

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)U3(1)	This command was introduced.

Usage Guidelines

Use the **ipv6 address** command to configure an IPv6 address or secondary address on an interface.

This command does not require a license.

Examples

This example shows how to configure an IPv6 address on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ipv6 address 2001:0DB8::1/8
switch(config-if)#
```

This example shows how to remove the IPv6 address configuration:

switch(config-if)# **no ipv6 address 2001:0DB8::1/8**

Related Commands

Command	Description
show ipv6 interface	Displays IPv6 information for an interface.

ipv6 access-list

To configure an IPv6 access control list (ACL) or to enter IPv6 access list configuration mode for a specific ACL, use the **ipv6 access-list** command. To remove the IPv6 ACL configuration, use the **no** form of this command.

ipv6 access-list {*acl-name* | **match-local-traffic**}

no ip6 access-list {*acl-name* | **match-local-traffic**}

Syntax Description

acl-name	Name of the IPv6 ACL. The ACL name can be any alphanumeric string up to 64 characters. The name cannot contain a space or quotation mark.
match-local-traffic	Enables the ACL to match all traffic inbound and outbound to or from the CPU.

Defaults

None

Command Modes

ACL configuration mode

Command History

Release	Modification
5.0(3)U3(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure an IPv6 ACL:

```
switch# configure terminal
switch(config)# ipv6 access-list ACL-1-IPv6
```

This example shows how to remove the IPv6 ACL configuration:

switch(config)# **no ipv6 access-list ACL-01-IPv6**

Related Commands

Command	Description
ipv6 traffic-filter	Configures access control for IPv6 packets.

ipv6 dhcp relay

To enable the DHCPv6 relay agent globally, use the **ipv6 dhcp relay** command. To globally disable this agent, use the **no** form of this command.

ipv6 dhcp relay

no ipv6 dhcp relay

Syntax Description

This command has no arguments or keywords.

Command Default

By default, this feature is globally disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)U1(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

Examples

This example shows how to globally enable the DHCPv6 relay agent:

```
switch# configure terminal
switch(config)# ipv6 dhcp relay
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
show ipv6 dhcp relay	Displays DHCPv6 relay configuration.
clear ipv6 dhcp relay statistics	Clears the DHCPv6 relay statistics.
show running-config dhcp	Displays DHCP snooping configuration.

ipv6 dhcp relay source-interface

To configure the source interface for the DHCPv6 relay agent globally, use the **ipv6 dhcp relay source-interface** command. To globally disable this agent, use the **no** form of this command.

ipv6 dhcp relay source-interface *interface*

no ipv6 dhcp relay source-interface *interface*

Syntax Description

interface	Name of the source interface.

Command Default

None.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)U1(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command. You must also enable the DHCPv6 relay agent using the **ipv6 dhcp relay** command.

Examples

This example shows how to globally configure the DHCPv6 relay source interface:

```
switch# configure terminal
switch(config)# ipv6 dhcp relay source-interface loopback 2
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ipv6 dhcp relay	Enables the DHCPv6 relay agent.
clear ipv6 dhcp relay statistics	Clears DHCPv6 relay statistics.
show ipv6 dhcp relay	Displays DHCPv6 relay configuration.
show running-config dhcp	Displays DHCP snooping configuration.

ipv6 traffic-filter

To configure access control for IPv6 packets, use the **ipv6 traffic-filter** command. To remove the access control configuration, use the **no** form of this command.

ipv6 traffic-filter *acl-name* [**in** | **out**]

no ipv6 traffic-filter *acl-name* [**in** | **out**]

Syntax Description

acl-name	Access Control List (ACL) name. An ACL name can be any alphanumeric string up to 64 characters.
in	(Optional) Specifies inbound packets.
out	(Optional) Specifies outbound packets.

Defaults

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)U3(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure ACL for IPv6 packets:

```
switch# configure terminal
switch(config)# ipv6 access-list ACL-1-IPv6
switch(config-ipv6-acl)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# interface ethernet 1/4
switch(config-if)# ipv6 traffic-filter ACL-1-IPv6 in
```

This example shows how to remove the IPv6 access control configuration:

```
switch(config-if)# no ipv6 traffic-filter ACL-1-IPv6 in
switch(config-if)#
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 access control list (ACL) or enters IPv6 ACL configuration mode.

ipv6 verify unicast source reachable-via

To configure Unicast reverse path forwarding (Unicast RPF) on an interface for IPv6, use the **ipv6 verify unicast source reachable-via** command.

ipv6 verify unicast source reachable-via {**any** | **rx**}

Syntax Description

any	Specifies a loose Unicast RPF.
rx	Specifies the strict Unicast RPF.

Defaults

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)U3(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure loose Unicast RPF for IPv6 packets:

```
switch# configure terminal
switch(config)# interface Ethernet 2/1
switch(config-if)# ipv6 address 2001:0DB8:c18:1::3/64
switch(config-if)# ipv6 verify unicast source reachable-via any
```

This example shows how configure strict Unicast RPF for IPv6 packets:

```
switch(config)# interface Ethernet 2/1
switch(config-if)# ipv6 address 2001:0DB8:c18:1::3/64
switch(config-if)# ipv6 verify unicast source reachable-via rx
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address on an interface.

ip verify unicast source reachable-via

To configure Unicast Reverse Path Forwarding (Unicast RPF) on an interface, use the **ip verify unicast source reachable-via** command. To remove Unicast RPF from an interface, use the **no** form of this command.

ip verify unicast source reachable-via {**any** [**allow-default**] | **rx**}

no ip verify unicast source reachable-via {**any** [**allow-default**] | **rx**}

Syntax Description

any	Specifies loose checking.
allow-default	(Optional) Specifies the MAC address to be used on the specified interface.
rx	Specifies strict checking.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

You can configure one of the following Unicast RPF modes on an ingress interface:

- Strict Unicast RPF mode—A strict mode check is successful when the following matches occur:
  - Unicast RPF finds a match in the Forwarding Information Base (FIB) for the packet source address.
  - The ingress interface through which the packet is received matches one of the Unicast RPF interfaces in the FIB match.

  If these checks fail, 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.

This command does not require a license.

Examples

This example shows how to configure loose Unicast RPF checking on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no switchport
switch(config-if)# ip verify unicast source reachable-via any
```

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

This example shows how to configure strict Unicast RPF checking on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# ip verify unicast source reachable-via rx
switch(config-if)#
```

Related Commands

Command	Description
show ip interface ethernet	Displays the IP-related information for an interface.
show running-config interface ethernet	Displays the interface configuration in the running configuration.
show running-config ip	Displays the IP configuration in the running configuration.

logging level acllog

To enable logging messages from ACLs and to configure the logging severity level, use the logging level **acllog** command. To remove the logging level acllog, use the **no** form of this command.

logging level acllog *severity-level*

no logging level acllog *severity-level*

Syntax Description

severity-level	Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows: • 0—emergency: System unusable • 1—alert: Immediate action needed • 2—critical: Critical condition • 3—error: Error condition • 4—warning: Warning condition • 5—notification: Normal but significant condition—default level • 6—informational: Informational message only (default) • 7—debugging: Appears during debugging only

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)U2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to set the acllog match-log-level to 6, informational:

```
switch# configure terminal
switch(config)# logging level acllog 6
switch(config)#
```

Related Commands

Command	Description
show logging level acllog	Displays logging messages and logging severity levels from ACLs.

mac port access-group

To apply a MAC access control list (ACL) to an interface, use the **mac port access-group** command. To remove a MAC ACL from an interface, use the **no** form of this command.

mac port access-group *access-list-name*

no mac port access-group *access-list-name*

Syntax Description

access-list-name	Name of the MAC ACL, which can be up to 64 alphanumeric, case-sensitive characters long.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

By default, no MAC ACLs are applied to an interface.

MAC ACLs apply to non-IP traffic.

You can use the **mac port access-group** command to apply a MAC ACL as a port ACL to the following interface types:

- Layer 2 interfaces
- Layer 2 EtherChannel interfaces

You can also apply a MAC ACL as a VLAN ACL. For more information, see the **match** command.

The switch applies MAC ACLs only to inbound traffic. When the switch applies a MAC ACL, the switch checks packets against the rules in the ACL. If the first matching rule permits the packet, the switch continues to process the packet. If the first matching rule denies the packet, the switch drops the packet and returns an ICMP host-unreachable message.

If you delete the specified ACL from the switch without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

Examples

This example shows how to apply a MAC ACL named mac-acl-01 to Ethernet interface 1/2:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# mac port access-group mac-acl-01
switch(config-if)#
```

This example shows how to remove a MAC ACL named mac-acl-01 from Ethernet interface 1/2:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no mac port access-group mac-acl-01
switch(config-if)#
```

Related Commands

Command	Description
show access-lists	Displays all ACLs.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.

match

To specify an access control list (ACL) for traffic filtering in a VLAN access map, use the **match** command. To remove a **match** command from a VLAN access map, use the **no** form of this command.

match {**ip** | **mac**} **address** *access-list-name*

no match {**ip** | **mac**} **address** *access-list-name*

Syntax Description

ip	Specifies an IPv4 ACL.
mac	Specifies a MAC ACL.
address *access-list-name*	Specifies the IPv4, IPv6, or MAC address and the access list name. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

By default, the switch classifies traffic and applies IPv4 ACLs to IPv4 traffic and MAC ACLs to all other traffic.

Command Modes

VLAN access-map configuration mode
Switch profile configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U2(1)	Support for this command was introduced in switch profiles.

Usage Guidelines

You can specify only one **match** command per access map.

Note The **ipv6** and **mac** keywords are not applicable in a VLAN access map configured in a switch profile.

Examples

This example shows how to create a VLAN access map named vlan-map-01, assign an IPv4 ACL named ip-acl-01 to the map, specify that the switch forwards packets matching the ACL, and enable statistics for traffic matching the map:

```
switch# configure terminal
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
switch(config-access-map)#
```

This example shows how to create a VLAN access map named vlan-map-03 in a switch profile, and assign an IPv4 ACL named ip-acl-03 to the map:

```
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)# vlan access-map vlan-map-03
switch(config-sync-sp-access-map)# match ip address ip-acl-03
switch(config-sync-sp-access-map)#
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.
show running-config switch-profile	Displays the running configuration for a switch profile.

permit (ARP)

To create an ARP ACL rule that permits ARP traffic that matches its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **permit ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac any**

no *sequence-number*

no permit ip {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac any**

Syntax Description

sequence-number	(Optional) Sequence number of the **permit** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
ip	Introduces the IP address portion of the rule.
any	Specifies that any host matches the part of the rule that contains the **any** keyword. You can use **any** to specify the sender IP address, target IP address, sender MAC address, and target MAC address.
host *sender-IP*	Specifies that the rules matches ARP packets only when the sender IP address in the packet matches the value of the *sender-IP* argument. Valid values for the *sender-IP* argument are IPv4 addresses in dotted-decimal format.
sender-IP sender-IP-mask	IPv4 address and mask for the set of IPv4 addresses that the sender IP address in the packet can match. The *sender-IP* and *sender-IP-mask* argument must be in dotted-decimal format. Specifying 255.255.255.255 as the *sender-IP-mask* argument is the equivalent of using the **host** keyword.
mac	Introduces the MAC address portion of the rule.

Command Default

None

Command Modes

ARP ACL configuration mode

Command History

Release	Modification
5.0(3)U2(1)	This command was introduced.

Usage Guidelines

Note As of Cisco NX-OS Release 5.0(3)U2(2), ARP access-list is supported only for Control Plane Policing (CoPP). The **permit** command is ignored for CoPP ARP ACLs.

A newly created ARP ACL contains no rules.

If you do not specify a sequence number, the device assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

When the device applies an ARP ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

Examples

This example shows how to enter ARP access list configuration mode for an ARP ACL named copp-arp-acl and add a rule that permits ARP request messages that will filter ARP packets coming from sender 192.0.32.14/24 subnet and associate them with the copp-arp-acl class:

```
switch# configure terminal
switch(config)# arp access-list copp-arp-acl
switch(config-arp-acl)# permit ip 192.0.32.14 255.255.255.0 mac any
switch(config-arp-acl)#
```

Related Commands

Command	Description
deny (ARP)	Configures a deny rule in an ARP ACL.
arp access-list	Configures an ARP ACL.
remark	Configures a remark in an ACL.
show arp access-lists	Displays all ARP ACLs or one ARP ACL.

permit (IPv4)

To create an IPv4 access control list (ACL) rule that permits traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **permit** *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**][**time-range** *time-range-name*]

no permit *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**][**time-range** *time-range-name*]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*] **permit icmp** *source destination* [*icmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**][**time-range** *time-range-name*]

Internet Group Management Protocol

[*sequence-number*] **permit igmp** *source destination* [*igmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**][**time-range** *time-range-name*]

Internet Protocol v4

[*sequence-number*] **permit ip** *source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**][**time-range** *time-range-name*]

Transmission Control Protocol

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**][**time-range** *time-range-name*] [*flags*] [**established**]

User Datagram Protocol

[*sequence-number*] **permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**][**time-range** *time-range-name*]

Syntax Description

sequence-number	(Optional) Sequence number of the **permit** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
protocol	Name or number of the protocol of packets that the rule matches. Valid numbers are from 0 to 255. Valid protocol names are the following keywords: • **ahp**—Specifies that the rule applies to authentication header protocol (AHP) traffic only. • **eigrp**—Specifies that the rule applies to Enhanced Interior Gateway Routing Protocol (EIGRP) traffic only. • **esp**—Specifies that the rule applies to IP Encapsulation Security Payload (ESP) traffic only. • **icmp**—Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **igmp**—Specifies that the rule applies to IGMP traffic only. When you use this keyword, the *igmp-type* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **ip**—Specifies that the rule applies to all IPv4 traffic. When you use this keyword, only the other keywords and arguments that apply to all IPv4 protocols are available. They include the following: – **dscp** – **fragments** – **log** – **precedence** – **time-range** • **nos**—Specifies that the rule applies to IP over IP encapsulation (KA9Q/NOS compatible) traffic only. • **ospf**— Specifies that the rule applies to Open Shortest Path First (OSPF) routing protocol traffic only. • **pcp**—Specifies that the rule applies to IP Payload Compression Protocol (IPComp) traffic only. • **pim**—Specifies that the rule applies to IPv4 Protocol Independent Multicast (PIM) traffic only.

	• **tcp**—Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **udp**—Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
source	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see "Source and Destination" in the "Usage Guidelines" section.
destination	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see "Source and Destination" in the "Usage Guidelines" section.
dscp *dscp*	(Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords: • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010. • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) • **af12**—AF class 1, medium drop probability (001100) • **af13**—AF class 1, high drop probability (001110) • **af21**—AF class 2, low drop probability (010010) • **af22**—AF class 2, medium drop probability (010100) • **af23**—AF class 2, high drop probability (010110) • **af31**—AF class 3, low drop probability (011010) • **af32**—AF class 3, medium drop probability (011100) • **af33**—AF class 3, high drop probability (011110) • **af41**—AF class 4, low drop probability (100010) • **af42**—AF class 4, medium drop probability (100100) • **af43**—AF class 4, high drop probability (100110) • **cs1**—Class-selector (CS) 1, precedence 1 (001000) • **cs2**—CS2, precedence 2 (010000) • **cs3**—CS3, precedence 3 (011000) • **cs4**—CS4, precedence 4 (100000) • **cs5**—CS5, precedence 5 (101000) • **cs6**—CS6, precedence 6 (110000) • **cs7**—CS7, precedence 7 (111000) • **default**—Default DSCP value (000000) • **ef**—Expedited Forwarding (101110)

precedence *precedence*	(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword as follows: • 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011. • **critical**—Precedence 5 (101) • **flash**—Precedence 3 (011) • **flash-override**—Precedence 4 (100) • **immediate**—Precedence 2 (010) • **internet**—Precedence 6 (110) • **network**—Precedence 7 (111) • **priority**—Precedence 1 (001) • **routine**—Precedence 0 (000)
fragments	(Optional) Specifies that the rule matches only those packets that are noninitial fragments. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the switch requires to evaluate those options is contained only in initial fragments.
time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command.
icmp-message	(Optional; IGMP only) Rule that matches only packets of the specified ICMP message type. This argument can be an integer from 0 to 255 or one of the keywords listed under “ICMP Message Types” in the “Usage Guidelines” section.
igmp-message	(Optional; IGMP only) Rule that matches only packets of the specified IGMP message type. The *igmp-message* argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords: • **dvmrp**—Distance Vector Multicast Routing Protocol • **host-query**—Host query • **host-report**—Host report • **pim**—Protocol Independent Multicast • **trace**—Multicast trace

operator port [*port*]	(Optional; TCP and UDP only) Rule that matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument must be one of the following keywords: • **eq**—Matches only if the port in the packet is equal to the *port* argument. • **gt**—Matches only if the port in the packet is greater than the *port* argument. • **lt**—Matches only if the port in the packet is less than the *port* argument. • **neq**—Matches only if the port in the packet is not equal to the *port* argument. • **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument.
portgroup *portgroup*	(Optional; TCP and UDP only) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. Use the **object-group ip port** command to create and change IP port-group objects.
flags	(Optional; TCP only) Rule that matches only packets that have specific TCP control bit flags set. The value of the *flags* argument must be one or more of the following keywords: • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	(Optional; TCP only) Specifies that the rule matches only packets that belong to an established TCP connection. The switch considers TCP packets with the ACK or RST bits set to belong to an established connection.

Command Default

A newly created IPv4 ACL contains no rules.

If you do not specify a sequence number, the device assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

Command Modes

IPv4 ACL configuration mode
IPv4 ACL in switch profile configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U2(1)	Support for this command was introduced in switch profiles. Support to include **any** or the **host** source address was introduced for IPv4 **permit ip** ACLs. Support was added for the following additional protocols: **ahp**, **eigrp**, **esp**, **nos**, **ospf**, **pcp**, and **pim**.

Usage Guidelines

When the switch applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  IPv4-address network-wildcard

  This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# permit tcp 192.168.67.0 0.0.0.255 any
  ```

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  IPv4-address/prefix-len

  This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# permit udp 192.168.67.0/24 any
  ```

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  host *IPv4-address*

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

This example shows how to specify the *source* argument with the **host** keyword and the 192.168.0.132 IPv4 address:

```
switch(config-acl)# permit icmp host 192.168.0.132 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

ICMP Message Types

The *icmp-message* argument can be the ICMP message number, which is an integer from 0 to 255. It can also be one of the following keywords:

- **administratively-prohibited**—Administratively prohibited
- **alternate-address**—Alternate address
- **conversion-error**—Datagram conversion
- **dod-host-prohibited**—Host prohibited
- **dod-net-prohibited**—Net prohibited
- **echo**—Echo (ping)
- **echo-reply**—Echo reply
- **general-parameter-problem**—Parameter problem
- **host-isolated**—Host isolated
- **host-precedence-unreachable**—Host unreachable for precedence
- **host-redirect**—Host redirect
- **host-tos-redirect**—Host redirect for ToS
- **host-tos-unreachable**—Host unreachable for ToS
- **host-unknown**—Host unknown
- **host-unreachable**—Host unreachable
- **information-reply**—Information replies
- **information-request**—Information requests
- **mask-reply**—Mask replies
- **mask-request**—Mask requests
- **mobile-redirect**—Mobile host redirect
- **net-redirect**—Network redirect
- **net-tos-redirect**—Net redirect for ToS
- **net-tos-unreachable**—Network unreachable for ToS
- **net-unreachable**—Net unreachable
- **network-unknown**—Network unknown
- **no-room-for-option**—Parameter required but no room
- **option-missing**—Parameter required but not present
- **packet-too-big**—Fragmentation needed and DF set
- **parameter-problem**—All parameter problems

- **port-unreachable**—Port unreachable
- **precedence-unreachable**—Precedence cutoff
- **protocol-unreachable**—Protocol unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—All redirects
- **router-advertisement**—Router discovery advertisements
- **router-solicitation**—Router discovery solicitations
- **source-quench**—Source quenches
- **source-route-failed**—Source route failed
- **time-exceeded**—All time-exceeded messages
- **timestamp-reply**—Time-stamp replies
- **timestamp-request**—Time-stamp requests
- **traceroute**—Traceroute
- **ttl-exceeded**—TTL exceeded
- **unreachable**—All unreachables

TCP Port Names

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

- **bgp**—Border Gateway Protocol (179)
- **chargen**—Character generator (19)
- **cmd**—Remote commands (rcmd, 514)
- **daytime**—Daytime (13)
- **discard**—Discard (9)
- **domain**—Domain Name Service (53)
- **drip**—Dynamic Routing Information Protocol (3949)
- **echo**—Echo (7)
- **exec**—EXEC (rsh, 512)
- **finger**—Finger (79)
- **ftp**—File Transfer Protocol (21)
- **ftp-data**—FTP data connections (2)
- **gopher**—Gopher (7)
- **hostname**—NIC hostname server (11)
- **ident**—Ident Protocol (113)
- **irc**—Internet Relay Chat (194)
- **klogin**—Kerberos login (543)
- **kshell**—Kerberos shell (544)
- **login**—Login (rlogin, 513)

- **lpd**—Printer service (515)
- **nntp**—Network News Transport Protocol (119)
- **pim-auto-rp**—PIM Auto-RP (496)
- **pop2**—Post Office Protocol v2 (19)
- **pop3**—Post Office Protocol v3 (11)
- **smtp**—Simple Mail Transport Protocol (25)
- **sunrpc**—Sun Remote Procedure Call (111)
- **tacacs**—TAC Access Control System (49)
- **talk**—Talk (517)
- **telnet**—Telnet (23)
- **time**—Time (37)
- **uucp**—Unix-to-Unix Copy Program (54)
- **whois**—WHOIS/NICNAME (43)
- **www**—World Wide Web (HTTP, 8)

UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

- **biff**—Biff (mail notification, comsat, 512)
- **bootpc**—Bootstrap Protocol (BOOTP) client (68)
- **bootps**—Bootstrap Protocol (BOOTP) server (67)
- **discard**—Discard (9)
- **dnsix**—DNSIX security protocol auditing (195)
- **domain**—Domain Name Service (DNS, 53)
- **echo**—Echo (7)
- **isakmp**—Internet Security Association and Key Management Protocol (5)
- **mobile-ip**—Mobile IP registration (434)
- **nameserver**—IEN116 name service (obsolete, 42)
- **netbios-dgm**—NetBIOS datagram service (138)
- **netbios-ns**—NetBIOS name service (137)
- **netbios-ss**—NetBIOS session service (139)
- **non500-isakmp**—Internet Security Association and Key Management Protocol (45)
- **ntp**—Network Time Protocol (123)
- **pim-auto-rp**—PIM Auto-RP (496)
- **rip**—Routing Information Protocol (router, in.routed, 52)
- **snmp**—Simple Network Management Protocol (161)
- **snmptrap**—SNMP Traps (162)
- **sunrpc**—Sun Remote Procedure Call (111)

- **syslog**—System Logger (514)
- **tacacs**—TAC Access Control System (49)
- **talk**—Talk (517)
- **tftp**—Trivial File Transfer Protocol (69)
- **time**—Time (37)
- **who**—Who service (rwho, 513)
- **xdmcp**—X Display Manager Control Protocol (177)

Examples

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules permitting all TCP and UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network:

```
switch# configure terminal
switch(config)# ip access-list acl-lab-01
switch(config-acl)# permit ip any host 10.176.0.0/16
switch(config-acl)# permit tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit udp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit tcp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit udp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)#
```

This example shows how to configure an IPv4 ACL named sp-acl in a switch profile with rules that permit all AHP and OSPF traffic from the 10.20.0.0 and 192.168.36.0 networks to the 10.172.0.0 network:

```
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)# ip access-list sp-acl
switch(config-sync-sp-acl)# permit ahp 10.20.0.0/16 10.172.0.0/16
switch(config-sync-sp-acl)# permit ospf 10.20.0.0/16 10.172.0.0/16
switch(config-sync-sp-acl)# permit ahp 192.168.36.0/16 10.172.0.0/16
switch(config-sync-sp-acl)# permit ospf 192.168.36.0/16 10.172.0.0/16
switch(config-sync-sp-acl)#
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
ip access-list	Configures an IPv4 ACL.
remark	Configures a remark in an ACL.
show ip access-lists	Displays all IPv4 ACLs or one IPv4 ACL.
show switch-profile	Displays information about the switch profile and the configuration revision.
switch-profile	Creates and configures a switch profile.

permit interface

To add interfaces for a user role interface policy, use the **permit interface** command. To remove interfaces, use the **no** form of this command.

permit interface *interface-list*

no permit interface

Syntax Description

interface-list	List of interfaces that the user role has permission to access.

Command Default

All interfaces

Command Modes

Interface policy configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

For permit interface statements to work, you need to configure a command rule to allow interface access, as shown in the following example:

```
switch(config-role)# rule number permit command configure terminal ; interface *
```

Examples

This example shows how to configure a range of interfaces for a user role interface policy:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/2 - 8
switch(config-role-interface)#
```

This example shows how to configure a list of interfaces for a user role interface policy:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/1, ethernet 1/3, ethernet 1/5
switch(config-role-interface)#
```

This example shows how to remove an interface from a user role interface policy:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# no permit interface ethernet 1/2
switch(config-role-interface)#
```

Related Commands

Command	Description
interface policy deny	Enters interface policy configuration mode for a user role.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

permit vlan

To add VLANs for a user role VLAN policy, use the **permit vlan** command. To remove VLANs, use the **no** form of this command.

permit vlan *vlan-list*

no permit vlan

Syntax Description

vlan-list	List of VLANs that the user role has permission to access.

Command Default

All VLANs

Command Modes

VLAN policy configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

For **permit vlan** statements to work, you need to configure a command **rule** to allow VLAN access, as shown in the following example:

```
switch(config-role)# rule number permit command configure terminal ; vlan *
```

Examples

This example shows how to configure a range of VLANs for a user role VLAN policy:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1-8
switch(config-role-vlan)#
```

This example shows how to configure a list of VLANs for a user role VLAN policy:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1, 10, 12, 20
switch(config-role-vlan)#
```

This example shows how to remove a VLAN from a user role VLAN policy:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# no permit vlan 2
switch(config-role-vlan)#
```

Related Commands

Command	Description
vlan policy deny	Enters VLAN policy configuration mode for a user role.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

permit vrf

To add virtual routing and forwarding instances (VRFs) for a user role VRF policy, use the **permit vrf** command. To remove VRFs, use the **no** form of this command.

permit vrf *vrf-list*

no permit vrf

Syntax Description

vrf-list	List of VRFs that the user role has permission to access.

Command Default

All VRFs

Command Modes

VRF policy configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to configure a range of VRFs for a user role VRF policy:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)# permit vrf management
switch(config-role-vrf)#
```

Related Commands

Command	Description
vrf policy deny	Enters VRF policy configuration mode for a user role.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

permit vsan

To permit access to a VSAN policy for a user role, use the **permit vsan** command. To revert to the default VSAN policy configuration for a user role, use the **no** form of this command.

permit vsan *vsan-list*

no permit vsan *vsan-list*

Syntax Description

vsan-list	Range of VSANs accessible to a user role. The range is from 1 to 4093. You can separate the range using the following separators: • **,** is a multirange separator; for example, 1-5, 10, 12, 100-201. • **-** is a range separator; for example, 101-201.

Command Default

None

Command Modes

User role configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

This command is enabled only after you deny a VSAN policy by using the **vsan policy deny** command.

Examples

This example shows how to permit access to a VSAN policy for a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# vsan policy deny
switch(config-role-vsan)# permit vsan 10, 12, 100-104
switch(config-role-vsan)#
```

Related Commands

Command	Description
vsan policy deny	Denies access to a VSAN policy for a user.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

radius-server deadtime

To configure the dead-time interval for all RADIUS servers on a Cisco Nexus 3000 Series switch, use the **radius-server deadtime** command. To revert to the default, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

Syntax Description

minutes	Number of minutes for the dead-time interval. The range is from 1 to 1440 minutes.

Command Default

0 minutes

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

The dead-time interval is the number of minutes before the switch checks a RADIUS server that was previously unresponsive.

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

Examples

This example shows how to configure the global dead-time interval for all RADIUS servers to perform periodic monitoring:

```
switch# configure terminal
switch(config)# radius-server deadtime 5
switch(config)#
```

This example shows how to revert to the default for the global dead-time interval for all RADIUS servers and disable periodic server monitoring:

```
switch# configure terminal
switch(config)# no radius-server deadtime 5
switch(config)#
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server directed-request

To allow users to send authentication requests to a specific RADIUS server when logging in, use the **radius-server directed request** command. To revert to the default, use the **no** form of this command.

radius-server directed-request

no radius-server directed-request

Syntax Description

This command has no arguments or keywords.

Command Default

Sends the authentication request to the configured RADIUS server group.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

You can specify the *username@vrfname:hostname* during login, where *vrfname* is the VRF to use and *hostname* is the name of a configured RADIUS server. The username is sent to the RADIUS server for authentication.

Examples

This example shows how to allow users to send authentication requests to a specific RADIUS server when logging in:

```
switch# configure terminal
switch(config)# radius-server directed-request
switch(config)#
```

This example shows how to disallow users to send authentication requests to a specific RADIUS server when logging in:

```
switch# configure terminal
switch(config)# no radius-server directed-request
switch(config)#
```

Related Commands

Command	Description
show radius-server directed-request	Displays the directed request RADIUS server configuration.

radius-server host

To configure RADIUS server parameters, use the **radius-server host** command. To revert to the default, use the **no** form of this command.

radius-server host {*hostname* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**] [**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*hostname* | *ipv4-address* | *pv6-address*} [**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**] [**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds* [**retransmit** *count*]]

Syntax Description

hostname	RADIUS server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
ipv4-address	RADIUS server IPv4 address in the ***A.B.C.D*** format.
ipv6-address	RADIUS server IPv6 address in the A:B::C:D format.
key	(Optional) Configures the RADIUS server preshared secret key.
0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.
shared-secret	Preshared key to authenticate communication between the RADIUS client and server. The preshared key can include any printable ASCII characters (white spaces are not allowed), is case sensitive, and has a maximum of 63 characters.
pac	(Optional) Enables the generation of Protected Access Credentials on the RADIUS Cisco ACS server for use with Cisco TrustSec.
accounting	(Optional) Configures accounting.
acct-port *port-number*	(Optional) Configures the RADIUS server port for accounting. The range is from 0 to 65535.
auth-port *port-number*	(Optional) Configures the RADIUS server port for authentication. The range is from 0 to 65535.
authentication	(Optional) Configures authentication.
retransmit *count*	(Optional) Configures the number of times that the switch tries to connect to a RADIUS server before reverting to local authentication. The range is from 1 to 5 times and the default is 1 time.
test	(Optional) Configures parameters to send test packets to the RADIUS server.
idle-time *time*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes.
password *password*	Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.

username *name*	Specifies a username in the test packets. The is alphanumeric, not case sensitive, and has a maximum of 32 characters.
timeout *seconds*	Specifies the timeout (in seconds) between retransmissions to the RADIUS server. The default is 1 second and the range is from 1 to 60 seconds.

Command Default

Accounting port: 1813

Authentication port: 1812

Accounting: enabled

Authentication: enabled

Retransmission count: 1

Idle-time: 0

Server monitoring: disabled

Timeout: 5 seconds

Test username: test

Test password: test

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Examples

This example shows how to configure RADIUS server authentication and accounting parameters:

```
switch# configure terminal
switch(config)# radius-server host 192.168.2.3 key HostKey
switch(config)# radius-server host 192.168.2.3 auth-port 2003
switch(config)# radius-server host 192.168.2.3 acct-port 2004
switch(config)# radius-server host 192.168.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 192.168.2.3 test idle-time 10
switch(config)# radius-server host 192.168.2.3 test username tester
switch(config)# radius-server host 192.168.2.3 test password 2B9ka5
switch(config)#
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server key

To configure a RADIUS shared secret key, use the **radius-server key** command. To remove a configured shared secret, use the **no** form of this command.

radius-server key [**0** | **7**] *shared-secret*

no radius-server key [**0** | **7**] *shared-secret*

Syntax Description

0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server.
7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the RADIUS client and server.
shared-secret	Preshared key used to authenticate communication between the RADIUS client and server. The preshared key can include any printable ASCII characters (white spaces are not allowed), is case sensitive, and has a maximum of 63 characters.

Command Default

Clear text authentication

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

You must configure the RADIUS preshared key to authenticate the switch to the RADIUS server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch. You can override this global key assignment by using the **key** keyword in the **radius-server host** command.

Examples

This example shows how to provide various scenarios to configure RADIUS authentication:

```
switch# configure terminal
switch(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(config)# radius-server key 7 public pac
switch(config)#
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server retransmit

To specify the number of times that the switch should try a request with a RADIUS server, use the **radius-server retransmit** command. To revert to the default, use the **no** form of this command.

radius-server retransmit *count*

no radius-server retransmit *count*

Syntax Description

count	Number of times that the switch tries to connect to a RADIUS server before reverting to local authentication. The range is from 1 to 5 times.

Command Default

1 retransmission

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to configure the number of retransmissions to RADIUS servers:

```
switch# configure terminal
switch(config)# radius-server retransmit 3
switch(config)#
```

This example shows how to revert to the default number of retransmissions to RADIUS servers:

```
switch# configure terminal
switch(config)# no radius-server retransmit 3
switch(config)#
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server timeout

To specify the time between retransmissions to the RADIUS servers, use the **radius-server timeout** command. To revert to the default, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout *seconds*

Syntax Description

seconds	Number of seconds between retransmissions to the RADIUS server. The range is from 1 to 60 seconds.

Command Default

1 second

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to configure the timeout interval:

```
switch# configure terminal
switch(config)# radius-server timeout 30
switch(config)#
```

This example shows how to revert to the default interval:

```
switch# configure terminal
switch(config)# no radius-server timeout 30
switch(config)#
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

remark

To enter a comment into an IPv4 or MAC access control list (ACL), use the **remark** command. To remove a remark command, use the **no** form of this command.

[*sequence-number*] **remark** *remark*

no {*sequence-number* | **remark** *remark*}

Syntax Description

sequence-number	(Optional) Sequence number of the **remark** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to remarks and rules.
remark	Text of the remark. This argument can be up to 100 characters.

Command Default

No ACL contains a remark by default.

Command Modes

ARP ACL configuration mode
IPv4 ACL configuration mode
IPv4 ACL in switch profile configuration mode
MAC ACL configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U2(1)	Support was extended for IPv4 ACLs in switch profiles, and Address Resolution Protocol (ARP) ACLs .

Usage Guidelines

The *remark* argument can be up to 100 characters. If you enter more than 100 characters for the *remark* argument, the switch accepts the first 100 characters and drops any additional characters.

Examples

This example shows how to create a remark in an IPv4 ACL and display the results:

```
switch# configure terminal
switch(config)# ip access-list acl-ipv4-01
switch(config-acl)# 100 remark this ACL denies the marketing department access to the lab
switch(config-acl)# show access-list acl-ipv4-01
```

```
switch(config-acl)#
```

This example shows how to create a remark in an IPv4 ACL in a switch profile:

```
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)# ip access-list sp-acl
switch(config-sync-sp-acl)# 30 remark this ACL permits TCP access to the Accounting team
switch(config-sync-sp-acl)#
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL.
ip access-list	Configures an IPv4 ACL.
show access-list	Displays all ACLs or one ACL.
show switch-profile	Displays information about the switch profile and the configuration revision.
switch-profile	Creates and configures a switch profile.

resequence

To reassign sequence numbers to all rules in an access control list (ACL) or a time range, use the **resequence** command.

resequence *access-list-type* **access-list** *access-list-name starting-number increment*

resequence time-range *time-range-name starting-number increment*

Syntax Description

access-list-type	Type of the ACL. Valid values for this argument are the following keywords: • **arp** **Note** This ACL type is not applicable to switch profiles. • **ip** • **mac**
access-list *access-list-name*	Specifies the name of the ACL. The ACL name can be a maximum of 64 alphanumeric characters.
time-range *time-range-name*	Specifies the name of the time range. **Note** This keyword is not applicable to switch profiles.
starting-number	Sequence number for the first rule in the ACL or time range. The range is from 1 to 4294967295.
increment	Number that the switch adds to each subsequent sequence number. The range is from 1 to 4294967295.

Command Default

None

Command Modes

Global configuration mode
Switch profile configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U2(1)	Support for this command was introduced in switch profiles.

Usage Guidelines

The **resequence** command allows you to reassign sequence numbers to the rules of an ACL or time range. The new sequence number for the first rule is determined by the *starting-number* argument. Each additional rule receives a new sequence number determined by the *increment* argument. If the highest sequence number would exceed the maximum possible sequence number, then no sequencing occurs and the following message appears:

```
ERROR: Exceeded maximum sequence number.
```

The maximum sequence number is 4294967295.

Examples

This example shows how to resequence an IPv4 ACL named ip-acl-01 with a starting sequence number of 100 and an increment of 10, using the **show ip access-lists** command to verify sequence numbering before and after the use of the **resequence** command:

```
switch# configure terminal
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        7 permit tcp 128.0.0/16 any eq www
        10 permit udp 128.0.0/16 any
        13 permit icmp 128.0.0/16 any eq echo
        17 deny igmp any any
switch(config)# resequence ip access-list ip-acl-01 100 10
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        100 permit tcp 128.0.0/16 any eq www
        110 permit udp 128.0.0/16 any
        120 permit icmp 128.0.0/16 any eq echo
        130 deny igmp any any
switch(config)#
```

This example shows how to resequence an IPv4 ACL named sp-acl in a switch profile with a starting sequence number of 30 and an increment of 5:

```
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)# resequence ip access-list sp-acl 30 5
switch(config-sync-sp)#
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL.
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs or a specific ACL.

role feature-group name

To create or specify a user role feature group and enter user role feature group configuration mode, use the **role feature-group name** command. To delete a user role feature group, use the **no** form of this command.

role feature-group name *group-name*

no role feature-group name *group-name*

Syntax Description

group-name	User role feature group name. The *group-name* has a maximum length of 32 characters and is a case-sensitive, alphanumeric character string.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to create a user role feature group and enter user role feature group configuration mode:

```
switch# configure terminal
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)#
```

This example shows how to remove a user role feature group:

```
switch# configure terminal
switch(config)# no role feature-group name MyGroup
switch(config)#
```

Related Commands

Command	Description
feature-group name	Specifies or creates a user role feature group and enters user role feature group configuration mode.
show role feature-group	Displays the user role feature groups.

role name

To create or specify a user role and enter user role configuration mode, use the **role name** command. To delete a user role, use the **no** form of this command.

role name {*role-name* | **default-role** | *privilege-role*}

no role name {*role-name* | **default-role** | *privilege-role*}

Syntax Description

role-name	User role name. The *role-name* has a maximum length of 16 characters and is a case-sensitive, alphanumeric character string.
default-role	Specifies the default user role name.
privilege-role	Privilege user role, which can be one of the following: • priv-0 • priv-1 • priv-2 • priv-3 • priv-4 • priv-5 • priv-6 • priv-7 • priv-8 • priv-9 • priv-10 • priv-11 • priv-12 • priv-13

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

A Cisco Nexus 3000 Series switch provides the following default user roles:

- Network Administrator—Complete read-and-write access to the entire switch
- Complete read access to the entire switch

You cannot change or remove the default user roles.

To view the privilege level roles, you must enable the cumulative privilege of roles for command authorization on TACACS+ servers using the **feature privilege** command. Privilege roles inherit the permissions of lower level privilege roles.

Examples

This example shows how to create a user role and enter user role configuration mode:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)#
```

This example shows how to create a privilege 1 user role and enter user role configuration mode:

```
switch# configure terminal
switch(config)# role name priv-1
switch(config-role)#
```

This example shows how to remove a user role:

```
switch# configure terminal
switch(config)# no role name MyRole
switch(config)#
```

Related Commands

Command	Description
feature privilege	Enables cumulative privilege of roles for command authorization on TACACS+ servers.
rule	Configures rules for user roles.
show role	Displays the user roles.

rule

To configure rules for a user role, use the **rule** command. To delete a rule, use the **no** form of this command.

rule *number* {**deny** | **permit**} {**command** *command-string* | {**read** | **read-write**} [**feature** *feature-name* | **feature-group** *group-name*]}

no rule *number*

Syntax Description

number	Sequence number for the rule. The switch applies the rule with the highest value first and then the rest in descending order.
deny	Denies access to commands or features.
permit	Permits access to commands or features.
command *command-string*	Specifies a command string. The command string can be a maximum of 128 characters and can contain spaces.
read	Specifies read access.
read-write	Specifies read and write access.
feature *feature-name*	(Optional) Specifies a feature name. Use the **show role feature** command to list the switch feature names.
feature-group *group-name*	(Optional) Specifies a feature group.

Command Default

None

Command Modes

User role configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

You can configure up to 256 rules for each role.

The rule number that you specify determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

Deny rules cannot be added to any privilege roles, except the privilege 0 (priv-0) role.

Examples

This example shows how to add rules to a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 1 permit read-write feature-group L3
```

```
switch(config-role)#
```

This example shows how to add rules to a user role with privilege 0:

```
switch# configure terminal
switch(config)# role name priv-0
switch(config-role)# rule 1 deny command clear users
switch(config-role)#
```

This example shows how to remove a rule from a user role:

```
switch# configure terminal
switch(config)# role MyRole
switch(config-role)# no rule 10
switch(config-role)#
```

Related Commands

Command	Description
role name	Creates or specifies a user role name and enters user role configuration mode.
show role	Displays the user roles.

server

To add a server to a RADIUS or TACACS+ server group, use the **server** command. To delete a server from a server group, use the **no** form of this command.

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

no server {*ipv4-address* | *hostname*}

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
ipv6-address	Server IPv6 address in the *X*:*X*:*X*::*X* format.
hostname	Server name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.

Command Default

None

Command Modes

RADIUS server group configuration mode
TACACS+ server group configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

You can configure up to 64 servers in a server group.

Use the **aaa group server radius** command to enter RADIUS server group configuration mode or **aaa group server tacacs+** command to enter TACACS+ server group configuration mode.

If the server is not found, use the **radius-server host** command or **tacacs-server host** command to configure the server.

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

Examples

This example shows how to add a server to a RADIUS server group:

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 192.168.1.1
switch(config-radius)#
```

This example shows how to delete a server from a RADIUS server group:

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)# no server 192.168.1.1
switch(config-radius)#
```

This example shows how to add a server to a TACACS+ server group:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 192.168.2.2
switch(config-tacacs+)#
```

This example shows how to delete a server from a TACACS+ server group:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no server 192.168.2.2
switch(config-tacacs+)#
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature tacacs+	Enables TACACS+.
radius-server host	Configures a RADIUS server.
show radius-server groups	Displays RADIUS server group information.
show tacacs-server groups	Displays TACACS+ server group information.
tacacs-server host	Configures a TACACS+ server.

show aaa accounting

To display authentication, authorization, and accounting (AAA) accounting configuration, use the **show aaa accounting** command.

show aaa accounting

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the configuration of the accounting log:

```
switch# show aaa accounting
```

Related Commands

Command	Description
aaa accounting default	Configures AAA methods for accounting.

show aaa authentication

To display authentication, authorization, and accounting (AAA) authentication configuration information, use the **show aaa authentication** command.

show aaa authentication login [**error-enable** | **mschap**]

Syntax Description

login	Displays the authentication login information.
error-enable	(Optional) Displays the authentication login error message enable configuration.
mschap	(Optional) Displays the authentication login Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) enable configuration.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the configured authentication parameters:

```
switch# show aaa authentication
```

This example shows how to display the authentication login error enable configuration:

```
switch# show aaa authentication login error-enable
```

This example shows how to display the authentication login MS-CHAP configuration:

```
switch# show aaa authentication login mschap
```

Related Commands

Command	Description
aaa authentication	Configures AAA authentication methods.

show aaa authorization

To display AAA authorization configuration information, use the **show aaa authorization** command.

show aaa authorization [**all**]

Syntax Description

all	(Optional) Displays configured and default values.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the configured authorization methods:

```
switch# show aaa authorization
```

Related Commands

Command	Description
aaa authorization commands default	Configures default AAA authorization methods for EXEC commands.
aaa authorization config-commands default	Configures default AAA authorization methods for configuration commands.

show aaa groups

To display authentication, authorization, and accounting (AAA) server group configuration, use the **show aaa groups** command.

show aaa groups

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display AAA group information:

```
switch# show aaa groups
```

Related Commands

Command	Description
aaa group server radius	Creates a RADIUS server group.

show aaa user

To display the status of the default role assigned by the authentication, authorization, and accounting (AAA) server administrator for remote authentication, use the **show aaa user** command.

show aaa user default-role

Syntax Description

default-role	Displays the status of the default AAA role.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the status of the default role assigned by the AAA server administrator for remote authentication:

```
switch# show aaa user default-role
```

Related Commands

Command	Description
aaa user default-role	Configures the default user for remote authentication.
show aaa authentication	Displays AAA authentication information.

show access-lists

To display all IPv4 and MAC access control lists (ACLs) or a specific ACL, use the **show access-lists** command.

show access-lists [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of an ACL, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

The switch shows all ACLs unless you use the *access-list-name* argument to specify an ACL.

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display all IPv4 and MAC ACLs on the switch that runs Cisco NX-OS Release 5.0(3)U2(1):

```
switch# show access-lists

IP access list copp-system-acl-icmp
        10 permit icmp any any
IP access list copp-system-acl-igmp
        10 permit igmp any any
IP access list copp-system-acl-ntp
        10 permit udp any any eq ntp
        20 permit udp any eq ntp any
IP access list copp-system-acl-ping
        10 permit icmp any any echo
        20 permit icmp any any echo-reply
IP access list copp-system-acl-routingproto1
        10 permit tcp any gt 1024 any eq bgp
        20 permit tcp any eq bgp any gt 1024
        30 permit udp any any eq rip
        40 permit tcp any gt 1024 any eq 639
        50 permit tcp any eq 639 any gt 1024
        60 permit eigrp any any
<--Output truncated-->
switch#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.

show accounting log

To display the accounting log contents, use the **show accounting log** command.

show accounting log [*size* | **all**] [**start-time** *year month day HH*:*MM*:*SS*] [**end-time** *year month day HH*:*MM*:*SS*]

Syntax Description

size	(Optional) Amount of the log to display in bytes. The range is from 0 to 250000.
all	(Optional) Specifies to display the entire accounting log.
start-time *year month day HH*:*MM*:*SS*	(Optional) Specifies a start time. The *year* argument is in *yyyy* format. The *month* is the three-letter English abbreviation. The *day* argument range is from 1 to 31. The *HH*:*MM*:*SS* argument is in standard 24-hour format.
end-time *year month day HH*:*MM*:*SS*	(Optional) Specifies an end time. The *year* argument is in *yyyy* format. The *month* is the three-letter English abbreviation. The *day* argument range is from 1 to 31. The *HH*:*MM*:*SS* argument is in standard 24-hour format.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U5(1e)	Show commands are included in the **show accounting log** command output after you enable terminal logging.

Examples

This example shows how to enable logging of all commands (including show comands) and how to display the entire accounting log:

```
switch# configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# terminal log-all
switch(config)# exit
switch# show accounting log all
Wed Apr  3 09:13:34 2013:type=update:id=console0:user=admin:cmd=configure terminal ;
terminal log-all (SUCCESS) >>>>>>>> new command configured
Wed Apr  3 09:13:42 2013:type=update:id=console0:user=admin:cmd=show accounting log all |
last 10 (SUCCESS)
Wed Apr  3 09:13:47 2013:type=update:id=console0:user=admin:cmd=show version (SUCCESS)
Wed Apr  3 09:13:53 2013:type=update:id=console0:user=admin:cmd=show accounting log all |
last 10 (SUCCESS)
Wed Apr  3 09:14:45 2013:type=start:id=64.103.217.184@pts/0:user=admin:cmd=
Wed Apr  3 09:14:48 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=show
running-config (SUCCESS)
Wed Apr  3 09:15:01 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=show
accounting log | last 10 (SUCCESS)
```

```
Wed Apr  3 09:15:07 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=show
accounting log all | last 10 (SUCCESS)
Wed Apr  3 09:17:14 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=show
accounting log all | last 10 (SUCCESS)
Wed Apr  3 09:17:21 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=show interface
brief (SUCCESS)
Wed Apr  3 09:17:27 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=show
accounting log all | last 10 (SUCCESS)
Wed Apr  3 09:17:49 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=configure
terminal ; interface Ethernet1/1/1-4 (SUCCESS)
Wed Apr  3 09:17:49 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=configure
terminal ; interface Ethernet1/1/1-4 ; shutdown (REDIRECT)
Wed Apr  3 09:17:50 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=configure
terminal ; interface Ethernet1/1/1-4 ; shutdown (SUCCESS)
Wed Apr  3 09:17:50 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=configure
terminal ; interface Ethernet1/1/1-4 ; shutdown (SUCCESS)
Wed Apr  3 09:17:50 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=configure
terminal ; interface Ethernet1/1/1-4 ; no shutdown (REDIRECT)
Wed Apr  3 09:17:50 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=configure
terminal ; interface Ethernet1/1/1-4 ; no shutdown (SUCCESS)
Wed Apr  3 09:17:50 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=configure
terminal ; interface Ethernet1/1/1-4 ; no shutdown (SUCCESS)
Wed Apr  3 09:17:57 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=show
accounting log all | last 20 (SUCCESS)
Wed Apr  3 09:20:11 2013:type=update:id=64.103.217.184@pts/0:user=admin:cmd=show system
internal ethpm info interface Ethernet1/1/1 (SUCCESS)
```

This example shows how to display 400 bytes of the accounting log on a switch that runs Cisco NX-OS Release 5.0(3)U2(1):

```
switch# show accounting log 400

Mon Aug  8 09:03:22 2011:type=update:id=console0:user=admin:cmd=setup (SUCCESS)
Tue Aug  9 06:19:03 2011:type=start:id=72.163.138.89@pts/0:user=admin:cmd=
Tue Aug  9 08:16:37 2011:type=start:id=console0:user=admin:cmd=
Tue Aug  9 08:17:21 2011:type=update:id=console0:user=admin:cmd=configure sync (
SUCCESS)
Tue Aug  9 08:17:25 2011:type=update:id=console0:user=admin:cmd=configure sync ;
 switch-profile s1 ; switch-profile s1 (SUCCESS)
switch#
```

This example shows how to display the accounting log starting at 16:00:00 on August 4, 2011:

```
switch# show accounting log start-time 2011 Aug 4 16:00:00

Fri Aug  5 04:03:55 2011:type=start:id=10.22.27.55@pts/3:user=admin:cmd=
Fri Aug  5 05:01:28 2011:type=stop:id=10.22.27.55@pts/3:user=admin:cmd=shell ter
minated because of telnet closed
Fri Aug  5 06:07:32 2011:type=start:id=console0:user=admin:cmd=
Fri Aug  5 06:11:27 2011:type=update:id=console0:user=admin:cmd=Erasing startup
configuration.
Fri Aug  5 06:11:27 2011:type=update:id=console0:user=admin:cmd=write erase (SUC
CESS)
Mon Aug  8 06:02:20 2011:type=update:id=console0:user=root:cmd=enabled (null)
Mon Aug  8 06:02:20 2011:type=update:id=console0:user=root:cmd=configure termina
l ; password strength-check (SUCCESS)
Mon Aug  8 06:02:20 2011:type=update:id=console0:user=root:cmd=updated v3 user :
 admin
Mon Aug  8 06:02:20 2011:type=update:id=console0:user=root:cmd=configure termina
l ; username admin password ******** role network-admin (SUCCESS)
Mon Aug  8 06:03:20 2011:type=update:id=console0:user=root:cmd=community public
set to read-only
<--Output truncated-->
switch#
```

This example shows how to display the accounting log starting at 15:59:59 on February 1, 2008 and ending at 16:00:00 on February 29, 2008:

```
switch# show accounting log start-time 2008 Feb 1 15:59:59 end-time 2008 Feb 29 16:00:00
```

Related Commands

Command	Description
clear accounting log	Clears the accounting log.
terminal log-all	Enables logging of all commands, including the **show** commands.

show arp access-lists

To display all ARP access control lists (ACLs) or a specific ARP ACL, use the **show arp access-lists** command.

show arp access-lists [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of an ARP ACL, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U2(1)	This command was introduced.

Usage Guidelines

The device shows all ARP ACLs, unless you use the *access-list-name* argument to specify an ACL.

This command does not require a license.

Examples

This example shows how to display all ARP ACLs on a switch:

```
switch# show arp access-lists

ARP access list copp-arp-acl
10 deny ip 192.0.32.14 255.255.255.0 mac any
20 permit ip 192.0.1.1 255.255.255.0 mac any
30 permit ip any mac any
40 permit ip host 192.0.32.14 mac any
switch#
```

This example shows how to display an ARP ACL named arp-permit-all:

```
switch# show arp access-lists arp-permit-all
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL.

show consistency-checker racl module

To trigger the RACL consistency checker for layer 3 interfaces in a module and display the results, use the **show consistency-checker racl module** command.

show consistency-checker racl module *slot*

Syntax Description

slot	Module number.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(3)U2(1)	This command was introduced.

Examples

This example shows how to trigger the RACL consistency checker for a module and display the results:

```
switch# show consistency-checker racl module 1
```

Related Commands

Command	Description
show consistency-checker l3-interface	Triggers the consistency checker on all interfaces in a module and displays the results.

show hardware profile tcam region

To display the access control list (ACL) ternary content addressable memory (TCAM) sizes that will be applicable after you reload the switch, use the **show hardware profile tcam region** command.

show hardware profile tcam region

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
7.0(3)I2(1)	The output for this command has changed.
5.0(3)U2(1)	This command was introduced.

Usage Guidelines

Use this command to see the new TCAM sizes you configured on the switch using the **hardware profile tcam region** command that will be applied after you reload the switch.

To see the current ACL TCAM sizes configured on the switch, use the **show platform afm info tcam** *asic-id* **region** {**arpacl** | **e-racl** | **e-vacl** | **ifacl** | **qos** | **racl** | **rbacl** | **span** | **sup** | **vacl**} command.

Note In Release 7.0(3)I2(1), the **show platform afm info tcam** command is being deprecated. The following two commands can be used instead to check for AFM/TCAM region outputs: **show hardware profile tcam region** and **show hardware access-list resource utilization**.

Examples

This example shows how to display the new TCAM entries:

```
switch# show hardware profile tcam region
   sup size =  128
  vacl size =  256
 ifacl size =  384
   qos size =  256
 rbacl size =    0
  span size =  128
  racl size =  256
e-racl size =  512
e-vacl size =  512
qoslbl size =  512
arpacl size =    0

switch#
```

This example shows how to display the new TCAM entries beginning in Release 7.0(3)I2(1):

```
switch# show hardware profile tcam region

TCAM Region Sizes:
                                  SUP Redirect size =  128
                               IPV4 VACL [vacl] size =  512
                              IPV4 PACL [ifacl] size =  384
                              IPV4 QOS [v4-qos] size =  256
                                           SPAN size =  128
                               IPV4 RACL [racl] size =  512
                       Egress IPV4 RACL [e-racl] size =  512
                                     IPV4 E-VACL size =  512
                                       QoS Label size =  256
                                            IPSG size =  256
                                       IPV6 RACL size =    0
                                     IPV6 E-RACL size =    0
                                          SUP V6 size =  256
                              IPV6 QOS [v6-qos] size =    0
                                   EGR QOS IPV4 size =    0
                                   EGR QOS IPV6 size =    0
                                    EGR QOS MAC size =    0
                              EGR QOS IPV4 LITE size =    0
                                        PBR IPV4 size =    0
                                        PBR IPV6 size =    0
                                         ARP ACL size =    0
switch#
```

Related Commands

Command	Description
show platform afm info tcam	Displays the current TCAM information.
hardware profile tcam region	Configures the sizes of the TCAM entries.

show ip access-lists

To display all IPv4 access control lists (ACLs) or a specific IPv4 ACL, use the **show ip access-lists** command.

show ip access-lists [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of an IPv4 ACL, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

The switch shows all IPv4 ACLs unless you use the *access-list-name* argument to specify an ACL.

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

By default, this command displays the IPv4 ACLs configured on the switch. The command displays the statistics information for an IPv4 ACL only if the IPv4 ACL is applied to the management (mgmt0) interface. If the ACL is applied to a switch virtual interface (SVI) or in a QoS class map, the command does not display any statistics information.

Examples

This example shows how to display all IPv4 ACLs on a switch that runs Cisco NX-OS release 5.0(3)U2(1):

```
switch# show ip access-lists

IP access list copp-system-acl-icmp
        10 permit icmp any any
IP access list copp-system-acl-igmp
        10 permit igmp any any
IP access list copp-system-acl-ntp
        10 permit udp any any eq ntp
        20 permit udp any eq ntp any
IP access list copp-system-acl-ping
        10 permit icmp any any echo
        20 permit icmp any any echo-reply
IP access list copp-system-acl-routingproto1
        10 permit tcp any gt 1024 any eq bgp
        20 permit tcp any eq bgp any gt 1024
        30 permit udp any any eq rip
        40 permit tcp any gt 1024 any eq 639
        50 permit tcp any eq 639 any gt 1024
        60 permit eigrp any any
<--Output truncated-->
switch#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs or a specific ACL.

show ip arp

To display the Address Resolution Protocol (ARP) table statistics, use the **show ip arp** command.

show ip arp [**detail** | **vlan** *vlan-id* [**vrf** {*vrf-name* | **all** | **default** | **management**}]]

Syntax Description

detail	(Optional) Displays the detailed ARP information.
vlan *vlan-id*	(Optional) Displays the ARP information for a specified VLAN. The range is from 1 to 4094, except for the VLANs reserved for internal use.
vrf	(Optional) Specifies the virtual routing and forwarding (VRF) to use.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Displays all VRF entries for the specified VLAN in the ARP table.
default	Displays the default VRF entry for the specified VLAN.
management	Displays the management VRF entry for the specified VLAN.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the ARP table:

```
switch# show ip arp
```

This example shows how to display the detailed ARP table:

```
switch# show ip arp detail
```

This example shows how to display the ARP table for VLAN 10 and all VRFs:

```
switch# show ip arp vlan 10 vrf all
```

Related Commands

Command	Description
clear ip arp	Clears the ARP cache and table.
show running-config arp	Displays the running ARP configuration.

show ip arp inspection

To display the Dynamic ARP Inspection (DAI) configuration status, use the **show ip arp inspection** command.

show ip arp inspection

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the status of the DAI configuration:

```
switch# show ip arp inspection
```

Related Commands

Command	Description
ip arp inspection vlan	Enables DAI for a specified list of VLANs.
show ip arp inspection interface	Displays the trust state and the ARP packet rate for a specified interface.
show ip arp inspection log	Displays the DAI log configuration.
show ip arp inspection statistics	Displays the DAI statistics.
show ip arp inspection vlan	Displays DAI status for a specified list of VLANs.
show running-config dhcp	Displays DHCP snooping configuration, including the DAI configuration.

show ip arp inspection interfaces

To display the trust state for the specified interface, use the **show ip arp inspection interfaces** command.

show ip arp inspection interfaces {**ethernet** *slot/port* | **port-channel** *channel-number*}

Syntax Description

ethernet *slot/port*	(Optional) Specifies that the output is for an Ethernet interface.
port-channel *channel-number*	(Optional) Specifies that the output is for a port-channel interface. Valid port-channel numbers are from 1 to 4096.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the trust state for a trusted interface:

```
switch# show ip arp inspection interfaces ethernet 2/1
```

Related Commands

Command	Description
ip arp inspection vlan	Enables Dynamic ARP Inspection (DAI) for a specified list of VLANs.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection vlan	Displays DAI status for a specified list of VLANs.
show running-config dhcp	Displays DHCP snooping configuration, including the DAI configuration.

show ip arp inspection log

To display the Dynamic ARP Inspection (DAI) log configuration, use the **show ip arp inspection log** command.

show ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the DAI log configuration:

```
switch# show ip arp inspection log
```

Related Commands

Command	Description
clear ip arp inspection log	Clears the DAI logging buffer.
ip arp inspection log-buffer	Configures the DAI logging buffer size.
show ip arp inspection	Displays the DAI configuration status.
show running-config dhcp	Displays DHCP snooping configuration, including the DAI configuration.

show ip arp inspection statistics

To display the Dynamic ARP Inspection (DAI) statistics, use the **show ip arp inspection statistics** command.

show ip arp inspection statistics [**vlan** *vlan-list*]

Syntax Description

vlan *vlan-list*	(Optional) Specifies the list of VLANs for which to display DAI statistics. Valid VLAN IDs are from 1 to 4094. You can specify a VLAN or range of VLANs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the DAI statistics for VLAN 1:

```
switch# show ip arp inspection statistics vlan 1
```

Related Commands

Command	Description
clear ip arp inspection statistics vlan	Clears the DAI statistics for a specified VLAN.
show ip arp inspection log	Displays the DAI log configuration.
show running-config dhcp	Displays DHCP snooping configuration, including the DAI configuration.

show ip arp inspection vlan

To display the Dynamic ARP Inspection (DAI) status for the specified list of VLANs, use the **show ip arp inspection vlan** command.

show ip arp inspection vlan *vlan-list*

Syntax Description

vlan-list	List of VLANs that have the DAI status. The *vlan-list* argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges. Valid VLAN IDs are from 1 to 4094.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the DAI status for VLAN 1:

```
switch# show ip arp inspection vlan 1
```

Related Commands

Command	Description
clear ip arp inspection statistics vlan	Clears the DAI statistics for a specified VLAN.
ip arp inspection vlan	Enables DAI for a specified list of VLANs.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection interface	Displays the trust state and the ARP packet rate for a specified interface.
show running-config dhcp	Displays DHCP snooping configuration, including the DAI configuration.

show ip dhcp snooping

To display general status information for Dynamic Host Configuration Protocol (DHCP) snooping, use the **show ip dhcp snooping** command.

show ip dhcp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display general status information about DHCP snooping:

```
switch# show ip dhcp snooping
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
ip dhcp snooping	Globally enables DHCP snooping on the device.
show ip dhcp snooping statistics	Displays DHCP snooping statistics.
show running-config dhcp	Displays the DHCP snooping configuration.

show ip dhcp snooping binding

To display IP-to-MAC address bindings for all interfaces or a specific interface, use the **show ip dhcp snooping binding** command.

show ip dhcp snooping binding [*IP-address*] [*MAC-address*] [**interface ethernet** *slot*/*port*] [**vlan** *vlan-id*]

show ip dhcp snooping binding [**dynamic**]

show ip dhcp snooping binding [**static**]

Syntax Description

IP-address	(Optional) IPv4 address that the bindings shown must include. Valid entries are in dotted-decimal format.
MAC-address	(Optional) MAC address that the bindings shown must include. Valid entries are in dotted-hexadecimal format.
interface ethernet *slot*/*port*	(Optional) Specifies the Ethernet interface that the bindings shown must be associated with. The slot number is from 1 to 255, and the port number is from 1 to 128.
vlan *vlan-id*	(Optional) Specifies a VLAN ID that the bindings shown must be associated with. Valid VLAN IDs are from 1 to 4094, except for the VLANs reserved for internal use. Use a hyphen (-) to separate the beginning and ending IDs of a range of VLAN IDs; for example, 70-100. Use a comma (,) to separate individual VLAN IDs and ranges of VLAN IDs; for example, 20,70-100,142.
dynamic	(Optional) Limits the output to all dynamic IP-MAC address bindings.
static	(Optional) Limits the output to all static IP-MAC address bindings.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

The binding interface includes static IP source entries. Static entries appear with the term “static” in the Type column.

Examples

This example shows how to show all bindings:

```
switch# show ip dhcp snooping binding
```

Related Commands

Command	Description
clear ip dhcp snooping binding	Clears the DHCP snooping binding database.
copy running-config startup-config	Copies the running configuration to the startup configuration.
ip dhcp snooping	Globally enables DHCP snooping on the device.
ip source binding	Creates a static IP source entry for a Layer 2 Ethernet interface.
show ip dhcp snooping statistics	Displays DHCP snooping statistics.
show running-config dhcp	Displays the DHCP snooping configuration.

show ip dhcp snooping statistics

To display Dynamic Host Configuration Protocol (DHCP) snooping statistics, use the **show ip dhcp snooping statistics** command.

show ip dhcp snooping statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display DHCP snooping statistics:

```
switch# show ip dhcp snooping statistics
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
ip dhcp snooping	Globally enables DHCP snooping on the device.
show running-config dhcp	Displays the DHCP snooping configuration.

show ipv6 dhcp relay

To display the configuration for the DHCPv6 relay agent, use the **show ipv6 dhcp relay** command.

show ipv6 dhcp relay [interface *interface***]**

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)U1(2)	This command was introduced.

Examples

This example shows how to display the configuration for the DHCPv6 relay agent:

```
switch# show ipv6 dhcp relay
```

Related Commands

Command	Description
ipv6 dhcp relay	Enables the DHCPv6 relay agent.
copy running-config startup-config	Copies the running configuration to the startup configuration.
show running-config dhcp	Displays the DHCP snooping configuration.

show ipv6 interface

To display IPv6 interface information for an interface, use the **show ipv6 interface** command.

show ipv6 interface [*ipv6-address* | **brief** | **detail** | **ethernet** | **loopback** | **mgmt** | **port-channel** | **vrf**]

Syntax Description

ipv6-address	(Optional) IPv6 address. The format is A:B::C:D/length. The length range is 1 to 128.
brief	(Optional) Displays a summary the of IPv6 status and configuration.
detail	(Optional) Displays the detailed IPv6 interface information.
ethernet	(Optional) Displays the Ethernet IEEE 802.3z.
loopback	(Optional) Displays the loopback interface.
mgmt	(Optional) Displays the management interface.
port-channel	(Optional) Displays the port channel interface.
vrf	(Optional) Displays information for each virtual routing and forwarding (VRF) instance.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U3(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display IPv6 information for an interface:

```
switch# show ipv6 interface
IPv6 Interface Status for VRF "default"
Ethernet1/8, Interface status: protocol-down/link-down/admin-up, iod: 14
  IPv6 address: 2001:db8:c18:1::3
  IPv6 subnet:  2001:db8:c18:1::/64
  IPv6 link-local address: fe80::205:73ff:feff:64ef (default)
  IPv6 virtual addresses configured: none
  IPv6 multicast routing: disabled
  IPv6 report link local: disabled
  IPv6 multicast groups locally joined:
      ff02::1:ff00:3  ff02::2  ff02::1  ff02::1:ffff:64ef
  IPv6 multicast (S,G) entries joined: none
  IPv6 MTU: 1500 (using link MTU)
  IPv6 unicast reverse path forwarding: none
  IPv6 load sharing: none
  IPv6 interface statistics last reset: never
```

```
  IPv6 interface RP-traffic statistics: (forwarded/originated/consumed)
    Unicast packets:      0/0/0
    Unicast bytes:        0/0/0
    Multicast packets:    0/0/0
    Multicast bytes:      0/0/0
switch(config-if)#
```

Related Commands

Command	Description
show ip interface	Displays IP information for an interface.

show ip verify source

To display the IP-to-MAC address bindings, use the **show ip verify source** command.

show ip verify source [**interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*}]

Syntax Description

interface	(Optional) Specifies that the output is limited to IP-to-MAC address bindings for a particular interface.
ethernet *slot*/*port*	(Optional) Specifies that the output is limited to bindings for the Ethernet interface given. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *channel-number*	(Optional) Specifies that the output is limited to bindings for the port-channel interface given. Valid port-channel numbers are from 1 to 4096.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U2(1)	This command was introduced.

Examples

This example shows how to display the IP-to-MAC address bindings on the switch:

```
switch# show ip verify source
```

Related Commands

Command	Description
ip source binding	Creates a static IP source entry for the specified Ethernet interface.
show running-config dhcp	Displays DHCP snooping configuration.

show logging ip access-list cache

To display the IP access list cache, use the **show logging ip access-list cache** command.

show logging ip access-list cache

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)U2(1)	This command was introduced.

Examples

This example shows how to display the status of the IP access list cache:

```
switch# show logging ip access-list cache
```

Related Commands

Command	Description
show logging ip access-list cache detail	Displays detailed information about the IP access list cache.
show logging ip access-list status	Displays the status of the IP access list cache.

show logging ip access-list status

To display the status of the IP access list cache, use the **show logging ip access-list status** command.

show logging ip access-list status

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)U2(1)	This command was introduced.

Examples

This example shows how to display the status of the IP access list cache:

```
switch# show logging ip access-list status
```

Related Commands

Command	Description
show logging ip access-list cache	Displays the IP access list cache.
show logging ip access-list cache detail	Displays detailed information about the IP access list cache.

show logging level acllog

To display logging messages and logging severity levels from ACLs, use the **show logging level acllog** command.

show logging level acllog

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
6.0(2)U2(1)	This command was introduced.

Examples

This example shows how to display the acllog match-log-level:

```
switch# show logging level acllog
```

Related Commands

Command	Description
logging level acllog	Enables logging messages from ACLs and configures the logging severity levels.

show platform afm info tcam

To display the platform-dependent access control list (ACL) Feature Manager (AFM) ternary content addressable memory (TCAM) driver information, use the **show platform afm info tcam** command.

Note In Release 7.0(3)I2(1), the **show platform afm info tcam** command is being deprecated. The following two commands can be used instead to check for AFM/TCAM region outputs: **show hardware profile tcam region** and **show hardware access-list resource utilization**.

show platform afm info tcam *asic-id* {{**bcm-entry** | **entry**} *low-tcam-index high-tcam-index* | **region** {**arpacl** | **e-racl** | **e-vacl** | **ifacl** | **qos** | **racl** | **rbacl** | **span** | **sup** | **vacl**}}

Syntax Description

asic-id	Global ASIC ID. The range is from 0 to 64.
bcm-entry	Displays BRCM TCAM entries within a range.
entry	Displays TCAM entries within a range.
low-tcam-index	Low TCAM index. The range is from 0 to 4095.
high-tcam-index	High TCAM index. The range is from 0 to 4095.
region	Displays TCAM information for a region.
arpacl	Displays TCAM information for an Address Resolution Protocol (ARP) ACL (ARPACL) region.
e-racl	Displays TCAM information for an egress router ACL (ERACL) region.
e-vacl	Displays TCAM information for an egress VLAN ACL (EVACL) region.
ifacl	Displays TCAM information for an interface ACL (IFACL) region.
qos	Displays TCAM information for a quality of service (QoS) region.
racl	Displays TCAM information for a router ACL (RACL) region.
rbacl	Displays TCAM information for a role based ACL (RBACL) region.
span	Displays TCAM information for a Switched Port Analyzer (SPAN) region.
sup	Displays TCAM information for a supervisor region.
vacl	Displays TCAM information for a VLAN ACL region.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
7.0(3)I2(1)	This command has been deprecated.
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the TCAM entries for the range 1 to 2 for ASIC ID 1:

```
switch# show platform afm info tcam 1 entry 1 2
TCAM entries in the range of 1 and 2 for asic id 1:
    K-keyType, L-label, B-bindcheck, DH-L2DA, CT-cdceTrnst
    L(IF-ifacl V-vacl Q-qos R-rbacl)

    [1]> K:IP (255/0) IN v4 L-[V-0/0 ]     [1]  SA:00000000/00000000
    [1]  DA:00000000/00000000
    [1]  L3Pr:ff/6 L4d:ffff/17(23)
    [1]-> prio:6  PERMIT    [1]  Result: Copy to CPU, code (1)    [1]  Result: C
osQNew (1)    StatsId = 1


    [2]> K:IP (255/0) IN v4 L-[V-0/0 ]     [2]  SA:00000000/00000000
    [2]  DA:00000000/00000000
    [2]  L3Pr:ff/6 L4d:ffff/50(80)
    [2]-> prio:6  PERMIT    [2]  Result: Copy to CPU, code (1)    [2]  Result: C
osQNew (1)    StatsId = 2


switch#
```

This example shows how to display the TCAM entries for an interface ACL region:

```
switch# show platform afm info tcam 1 region ifacl
ifacl tcam TCAM configuration for asic id 1:
[  sup tcam]: range     0 -  127
[ vacl tcam]: range   128 -  639
[ifacl tcam]: range   640 - 1023 *
[  qos tcam]: range  1024 - 1279
[rbacl tcam]: range     0 -    0
[ span tcam]: range  1280 - 1407
[ racl tcam]: range  1408 - 1919
[eracl tcam]: range  1920 - 2431
[evacl tcam]: range  2432 - 2943
[qoslbl tcam]: range  2944 - 3967

    TCAM [ifacl tcam]: [v:1, size:384, start:640 end:1023]
    In use tcam entries: 6
        640-645

switch#
```

Related Commands

Command	Description
show tech-support	Displays information for Cisco technical support.

show privilege

To show the current privilege level, username, and status of cumulative privilege support, use the **show privilege** command.

show privilege

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

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

Examples

This example shows how to view the current privilege level, username, and status of cumulative privilege support:

```
switch# show privilege
```

Related Commands

Command	Description
enable	Enables a user to move to a higher privilege level.
enable secret priv-lvl	Enables a secret password for a specific privilege level.
feature privilege	Enables the cumulative privilege of roles for command authorization on RADIUS and TACACS+ servers.
username	Enables a user to use privilege levels for authorization.

show radius-server

To display RADIUS server information, use the **show radius-server** command.

show radius-server [*hostname* | *ipv4-address*| *ipv6-address*] [**directed-request** | **groups** [*group-name*] | **sorted** | **statistics** *hostname* | *ipv4-address*]

Syntax Description

hostname	(Optional) RADIUS server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
ipv4-address	(Optional) RADIUS server IPv4 address in the *A*.*B*.*C*.*D* format.
ipv6-address	(Optional) RADIUS server IPv6 address in the *A*:*B*::*C*:*D* format.
directed-request	(Optional) Displays the directed request configuration.
groups	(Optional) Displays information about the configured RADIUS server groups.
group-name	RADIUS server group.
sorted	(Optional) Displays sorted-by-name information about the RADIUS servers.
statistics	(Optional) Displays RADIUS statistics for the RADIUS servers. A hostname or IP address is required.

Command Default

Displays the global RADIUS server configuration.

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

RADIUS preshared keys are not visible in the **show radius-server** command output. Use the **show running-config radius** command to display the RADIUS preshared keys.

Examples

This example shows how to display information for all RADIUS servers:

```
switch# show radius-server
```

This example shows how to display information for a specified RADIUS server:

```
switch# show radius-server 192.168.1.1
```

This example shows how to display the RADIUS directed request configuration:

```
switch# show radius-server directed-request
```

This example shows how to display information for RADIUS server groups:

```
switch# show radius-server groups
```

This example shows how to display information for a specified RADIUS server group:

```
switch# show radius-server groups RadServer
```

This example shows how to display sorted information for all RADIUS servers:

```
switch# show radius-server sorted
```

This example shows how to display statistics for a specified RADIUS servers:

```
switch# show radius-server statistics 192.168.1.1
```

Related Commands

Command	Description
show running-config radius	Displays the RADIUS information in the running configuration file.

show role

To display the user role configuration, use the **show role** command.

show role [**name** *role-name*]

Syntax Description

name *role-name*	(Optional) Displays information for a specific user role name.

Command Default

Displays information for all user roles.

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display information for a specific user role:

```
switch# show role name MyRole
```

This example shows how to display information for all user roles:

```
switch# show role
```

Related Commands

Command	Description
role name	Configures user roles.

show role feature

To display the user role features, use the **show role feature** command.

show role feature [**detail** | **name** *feature-name*]

Syntax Description

detail	(Optional) Displays detailed information for all features.
name *feature-name*	(Optional) Displays detailed information for a specific feature. The name can be a maximum of 16 alphanumeric characters and is case sensitive.

Command Default

Displays a list of user role feature names.

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the user role features:

```
switch# show role feature
```

This example shows how to display detailed information all the user role features:

```
switch# show role feature detail
```

This example shows how to display detailed information for a specific user role feature named arp:

```
switch# show role feature name arp
```

Related Commands

Command	Description
role feature-group	Configures feature groups for user roles.
rule	Configures rules for user roles.

show role feature-group

To display the user role feature groups, use the **show role feature-group** command.

show role feature-group [**detail** | **name** *group-name*]

Syntax Description

detail	(Optional) Displays detailed information for all feature groups.
name *group-name*	(Optional) Displays detailed information for a specific feature group.

Command Default

Displays a list of user role feature groups.

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the user role feature groups:

```
switch# show role feature-group
```

This example shows how to display detailed information about all the user role feature groups:

```
switch# show role feature-group detail
```

This example shows how to display information for a specific user role feature group:

```
switch# show role feature-group name SecGroup
```

Related Commands

Command	Description
role feature-group	Configures feature groups for user roles.
rule	Configures rules for user roles.

show running-config aaa

To display authentication, authorization, and accounting (AAA) configuration information in the running configuration, use the **show running-config aaa** command.

show running-config aaa [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the configured AAA information in the running configuration:

```
switch# show running-config aaa
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running system configuration to the startup configuration file.

show running-config acllog

To display the access control list (ACL) log file in the running configuration, use the **show running-config acllog** command.

show running-config acllog [all]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)U2(1)	This command was introduced.

Examples

This example displays the access control list (ACL) log in the running configuration:

```
switch# show running-config acllog [all]
```

Related Commands

Command	Description
show startup-config acllog	Displays the startup configuration of the ACL log file.

show running-config aclmgr

To display the access control list (ACL) configuration in the running configuration, use the **show running-config aclmgr** command.

show running-config aclmgr [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U2(1)	Support for this command was introduced for Control Plane Policing (CoPP).

Examples

This example shows how to display the ACL running configuration on a switch that runs Cisco NX-OS Release 5.0(3)U2(1):

```
switch# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Tue Aug 23 06:28:15 2011

version 5.0(3)U2(1)
ip access-list copp-system-acl-eigrp
  10 permit eigrp any 224.0.0.10/32
ip access-list copp-system-acl-icmp
  10 permit icmp any any
ip access-list copp-system-acl-igmp
  10 permit igmp any any
ip access-list copp-system-acl-ntp
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
ip access-list copp-system-acl-pimreg
<--Output truncated-->
switch#
```

This example shows how to display only the VTY running configuration:

```
switch# show running-config aclmgr | begin vty
```

Related Commands

Command	Description
access-class	Configures access classes for VTY.
control-plane	Enters the control-plane configuration mode.
copy running-config startup-config	Copies the running configuration to the startup configuration file.
ip access-class	Configures IPv4 access classes for VTY.
ipv6 access-class	Configures IPv6 access classes for VTY.
show startup-config aclmgr	Displays the ACL startup configuration.

show running-config arp

To display the Address Resolution Protocol (ARP) configuration in the running configuration, use the **show running-config arp** command.

show running-config arp [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the ARP configuration:

```
switch# show running-config arp
```

This example shows how to display the ARP configuration with the default information:

```
switch# show running-config arp all
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration file.
ip arp event-history errors	Logs ARP debug events into the event history buffer.
ip arp timeout	Configures an ARP timeout.
ip arp inspection	Displays general information about DHCP snooping.
show startup-config arp	Displays the ARP startup configuration.

show running-config dhcp

To display the Dynamic Host Configuration Protocol (DHCP) snooping configuration in the running configuration, use the **show running-config dhcp** command.

show running-config dhcp [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

Examples

This example shows how to display the DHCP snooping configuration:

```
switch# show running-config dhcp
```

This example shows how to display the DHCP snooping configuration with the default information:

```
switch# show running-config dhcp all
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping	Globally enables DHCP snooping on the device.
show ip dhcp snooping	Displays general information about DHCP snooping.
show startup-config dhcp	Displays the DHCP startup configuration.

show running-config radius

To display RADIUS server information in the running configuration, use the **show running-config radius** command.

show running-config radius [**all**]

Syntax Description

all	(Optional) Displays default RADIUS configuration information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display information for RADIUS in the running configuration:

```
switch# show running-config radius
```

Related Commands

Command	Description
show radius-server	Displays RADIUS information.

show running-config security

To display user account, Secure Shell (SSH) server, and Telnet server information in the running configuration, use the **show running-config security** command.

show running-config security [**all**]

Syntax Description

all	(Optional) Displays default user account, SSH server, and Telnet server configuration information.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display user account, SSH server, and Telnet server information in the running configuration:

```
switch# show running-config security
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running system configuration to the startup confguration file.

show ssh key

To display the Secure Shell (SSH) server key, use the **show ssh key** command.

show ssh key

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

This command is available only when SSH is enabled using the **ssh server enable** command.

Examples

This example shows how to display the SSH server key:

```
switch# show ssh key
```

Related Commands

Command	Description
ssh server key	Configures the SSH server key.

show ssh server

To display the Secure Shell (SSH) server status, use the **show ssh server** command.

show ssh server

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the SSH server status:

```
switch# show ssh server
```

Related Commands

Command	Description
ssh server enable	Enables the SSH server.

show startup-config aaa

To display authentication, authorization, and accounting (AAA) configuration information in the startup configuration, use the **show startup-config aaa** command.

show startup-config aaa

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the AAA information in the startup configuration:

```
switch# show startup-config aaa
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running system configuration to the startup confguration file.

show startup-config acllog

To display the access control list (ACL) log file in the startup configuration, use the **show startup-config acllog** command.

show startup-config acllog [all]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)U2(1)	This command was introduced.

Examples

This example displays the startup configuration for the ACL log:

```
switch# show startup-config acllog [all]
```

Command	Description
show running-config acllog	Displays the running configuration of the ACL log file.

show startup-config aclmgr

To display the access control list (ACL) configuration in the startup configuration, use the **show startup-config aclmgr** command.

show startup-config aclmgr [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the ACL startup configuration:

```
switch# show startup-config aclmgr

!Command: show startup-config aclmgr
!Time: Tue Aug 23 07:16:55 2011
!Startup config saved at: Sat Aug 20 04:58:59 2011

version 5.0(3)U2(1)
ip access-list copp-system-acl-eigrp
  10 permit eigrp any 224.0.0.10/32
ip access-list copp-system-acl-icmp
  10 permit icmp any any
ip access-list copp-system-acl-igmp
  10 permit igmp any any
ip access-list copp-system-acl-ntp
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
ip access-list copp-system-acl-pimreg
  10 permit pim any any
ip access-list copp-system-acl-ping
  10 permit icmp any any echo
  20 permit icmp any any echo-reply
<--Output truncated-->
switch#
```

This example shows how to display only the VTY startup configuration:

```
switch# show startup-config aclmgr | begin vty
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration file.
show running-config aclmgr	Displays the ACL running configuration.

show startup-config arp

To display the Address Resolution Protocol (ARP) configuration in the startup configuration, use the **show startup-config arp** command.

show startup-config arp [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the ARP startup configuration:

```
switch# show startup-config arp
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration file.
ip arp event-history errors	Logs ARP debug events into the event history buffer.
ip arp timeout	Configures an ARP timeout.
ip arp inspection	Displays general information about DHCP snooping.
show running-config arp	Displays the ARP running configuration.

show startup-config dhcp

To display the Dynamic Host Configuration Protocol (DHCP) snooping configuration in the startup configuration, use the **show running-config dhcp** command.

show running-config dhcp [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

Examples

This example shows how to display the DHCP snooping configuration in the startup configuration file:

```
switch# show startup-config dhcp
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
feature dhcp	Enables the DHCP snooping feature on the device.
show running-config dhcp	Displays the DHCP running configuration.

show startup-config radius

To display RADIUS configuration information in the startup configuration, use the **show startup-config radius** command.

show startup-config radius

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the RADIUS information in the startup configuration:

```
switch# show startup-config radius
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running system configuration to the startup confguration file.

show startup-config security

To display user account, Secure Shell (SSH) server, and Telnet server configuration information in the startup configuration, use the **show startup-config security** command.

show startup-config security

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the user account, SSH server, and Telnet server information in the startup configuration:

```
switch# show startup-config security
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running system configuration to the startup confguration file.

show tacacs-server

To display TACACS+ server information, use the **show tacacs-server** command.

show tacacs-server [*hostname* | *ip4-address* | *ip6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]

Syntax Description

hostname	(Optional) TACACS+ server Domain Name Server (DNS) name. The maximum character size is 256.
ipv4-address	(Optional) TACACS+ server IPv4 address in the *A.B.C.D* format.
ipv6-address	(Optional) TACACS+ server IPv6 address in the *X:X:X::X* format.
directed-request	(Optional) Displays the directed request configuration.
groups	(Optional) Displays information about the configured TACACS+ server groups.
sorted	(Optional) Displays sorted-by-name information about the TACACS+ servers.
statistics	(Optional) Displays TACACS+ statistics for the TACACS+ servers.

Command Default

Displays the global TACACS+ server configuration.

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

TACACS+ preshared keys are not visible in the **show tacacs-server** command output. Use the **show running-config tacacs+** command to display the TACACS+ preshared keys.

You must use the **feature tacacs+** command before you can display TACACS+ information.

Examples

This example shows how to display information for all TACACS+ servers:

```
switch# show tacacs-server
```

This example shows how to display information for a specified TACACS+ server:

```
switch# show tacacs-server 192.168.2.2
```

This example shows how to display the TACACS+ directed request configuration:

```
switch# show tacacs-server directed-request
```

This example shows how to display information for TACACS+ server groups:

```
switch# show tacacs-server groups
```

This example shows how to display information for a specified TACACS+ server group:

```
switch# show tacacs-server groups TacServer
```

This example shows how to display sorted information for all TACACS+ servers:

```
switch# show tacacs-server sorted
```

This example shows how to display statistics for a specified TACACS+ server:

```
switch# show tacacs-server statistics 192.168.2.2
```

Related Commands

Command	Description
show running-config tacacs+	Displays the TACACS+ information in the running configuration file.

show telnet server

To display the Telnet server status, use the **show telnet server** command.

show telnet server

Note Beginning in Release 7.0(3)I2(1), the error message displayed has changed from "telnet service not enabled" to "Telnet service is disabled."

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
7.0(3)I2(1)	An error message changed.
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display the Telnet server status:

```
switch# show telnet server
```

Related Commands

Command	Description
telnet server enable	Enables the Telnet server.

show user-account

To display information about the user accounts on the switch, use the **show user-account** command.

show user-account [*name*]

Syntax Description

name	(Optional) Information about the specified user account only.

Command Default

Displays information about all the user accounts defined on the switch.

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display information about all the user accounts defined on the switch:

```
switch# show user-account
```

This example shows how to display information about a specific user account:

```
switch# show user-account admin
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running system configuration to the startup confguration file.

show users

To display the users currently logged on the switch, use the **show users** command.

show users

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display all the users currently logged on the switch:

```
switch# show users
```

Related Commands

Command	Description
clear user	Logs out a specific user.
username	Creates and configures a user account.

show vlan access-list

To display the contents of the IPv4 access control list (ACL) or MAC ACL associated with a specific VLAN access map, use the **show vlan access-list** command.

show vlan access-list *map-name*

Syntax Description

map-name	VLAN access list to show.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

For the specified VLAN access map, the switch displays the access map name and the contents of the ACL associated with the map.

Examples

This example shows how to display the contents of the ACL associated with the specified VLAN access map:

```
switch# show vlan access-list vlan1map
```

Related Commands

Command	Description
ip access-list	Creates or configures an IPv4 ACL.
show access-lists	Displays information about how a VLAN access map is applied.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
vlan access-map	Configures a VLAN access map.

show vlan access-map

To display all VLAN access maps or a VLAN access map, use the **show vlan access-map** command.

show vlan access-map [*map-name*]

Syntax Description

map-name	(Optional) VLAN access map to show.

Command Default

The switch shows all VLAN access maps, unless you use the *map-name* argument to select a specific access map.

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

For each VLAN access map displayed, the switch shows the access map name, the ACL specified by the **match** command, and the action specified by the **action** command.

Use the **show vlan filter** command to see which VLANs have a VLAN access map applied to them.

Examples

This example shows how to display a specific VLAN access map:

```
switch# show vlan access-map vlan1map
```

This example shows how to display all VLAN access maps:

```
switch# show vlan access-map
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

show vlan filter

To display information about instances of the **vlan filter** command, including the VLAN access map and the VLAN IDs affected by the command, use the **show vlan filter** command.

show vlan filter [**access-map** *map-name* | **vlan** *vlan-id*]

Syntax Description

access-map *map-name*	(Optional) Limits the output to VLANs that the specified access map is applied to.
vlan *vlan-id*	(Optional) Limits the output to access maps that are applied to the specified VLAN only.

Command Default

All instances of VLAN access maps applied to a VLAN are displayed, unless you use the **access-map** keyword and specify an access map or you use the **vlan** keyword and specify a VLAN ID.

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to display all VLAN access map information on the switch:

```
switch# show vlan filter
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

ssh6

To create a Secure Shell (SSH) session using IPv6, use the **ssh6** command.

ssh6 [*username@*]{*ipv6-address* | *hostname*} [**vrf** {*vrf-name* | **default** | *management*}]

Syntax Description

username	(Optional) Username for the SSH session. The username is not case sensitive and has a maximum of 64 characters.
ipv6-address	IPv6 address of the remote host.
hostname	Hostname of the remote host. The hostname is case sensitive and has a maximum of 64 characters.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the SSH IPv6 session. The name can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

Default VRF

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

The switch supports SSH version 1 and 2.

Examples

This example shows how to start an SSH session using IPv6:

```
switch# ssh6 2001:0DB8::200C:417A vrf management
```

Related Commands

Command	Description
clear ssh session	Clears SSH sessions.
ssh	Starts an SSH session using IPv4 addressing.
ssh server enable	Enables the SSH server.

ssh

To create a Secure Shell (SSH) session using IPv4, use the **ssh** command.

ssh [*username*@]{*ipv4-address* | *hostname*} [**vrf** {*vrf-name* | **default** | **management**}]

Syntax Description

username	(Optional) Username for the SSH session. The username is not case sensitive and has a maximum of 64 characters.
ipv4-address	IPv4 address of the remote host.
hostname	Hostname of the remote host. The hostname is case sensitive and has a maximum of 64 characters.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the SSH session. The name can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

Default VRF

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

The switch supports SSH version 1 and 2.

Examples

This example shows how to start an SSH session using IPv4:

```
switch# ssh 192.168.1.1 vrf management
```

Related Commands

Command	Description
clear ssh session	Clears SSH sessions.
ssh server enable	Enables the SSH server.
ssh6	Starts an SSH session using IPv6 addressing.

ssh key

To create a Secure Shell (SSH) server key, use the **ssh key** command. To remove the SSH server key, use the **no** form of this command.

ssh key {**dsa** [**force**] | **rsa** [*length* [**force**]]}

no ssh key [**dsa** | **rsa**]

Syntax Description

dsa	Specifies the Digital System Algorithm (DSA) SSH server key.
force	(Optional) Forces the generation of a DSA SSH key even if previous ones are present.
rsa	Specifies the Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key.
length	(Optional) Number of bits to use when creating the SSH server key. The range is from 768 to 2048.

Command Default

1024-bit length

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software supports SSH version 1 and 2.

If you want to remove or replace an SSH server key, you must first disable the SSH server using the **no ssh server enable** command.

Examples

This example shows how to create an SSH server key using RSA with the default key length:

```
switch# configure terminal
switch(config)# ssh key rsa
switch(config)#
```

This example shows how to create an SSH server key using RSA with a specified key length:

```
switch# configure terminal
switch(config)# ssh key rsa 768
switch(config)#
```

This example shows how to replace an SSH server key using DSA with the force option:

```
switch# configure terminal
switch(config)# no ssh server enable
switch(config)# ssh key dsa force
switch(config)# ssh server enable
```

```
switch(config)#
```

This example shows how to remove the DSA SSH server key:

```
switch# configure terminal
switch(config)# no ssh server enable
switch(config)# no ssh key dsa
switch(config)# ssh server enable
switch(config)#
```

This example shows how to remove all SSH server keys:

```
switch# configure terminal
switch(config)# no ssh server enable
switch(config)# no ssh key
switch(config)# ssh server enable
switch(config)#
```

Related Commands

Command	Description
show ssh key	Displays the SSH server key information.
ssh server enable	Enables the SSH server.

ssh server enable

To enable the Secure Shell (SSH) server, use the **ssh server enable** command. To disable the SSH server, use the **no** form of this command.

ssh server enable

no ssh server enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

The switch supports SSH version 1 and 2.

Examples

This example shows how to enable the SSH server:

```
switch(config)# ssh server enable
```

This example shows how to disable the SSH server:

```
switch(config)# no ssh server enable
```

Related Commands

Command	Description
show ssh server	Displays the SSH server key information.

statistics per-entry

To start recording statistics for how many packets are permitted or denied by each entry in a VLAN access map, use the **statistics per-entry** command. To stop recording per-entry statistics, use the **no** form of this command.

statistics per-entry

no statistics per-entry

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

VLAN access-map configuration mode
Switch profile VLAN access-map configuration mode

Command History

Release	Modification
5.0(3)U2(1)	This command was introduced.

Usage Guidelines

Statistics are not supported if the DHCP snooping feature is enabled.

Examples

This example shows how to start recording per-entry statistics for a VLAN access map named vlan-map-01:

```
switch# configure terminal
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# statistics per-entry
switch(config-access-map)#
```

This example shows how to start recording per-entry statistics for a VLAN access map named vlan-map-03 in a switch profile:

```
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)# vlan access-map vlan-map-03
switch(config-sync-sp-access-map)# statistics per-entry
switch(config-sync-sp-access-map)#
```

This example shows how to stop recording per-entry statistics for a VLAN access map named vlan-map-03 in a switch profile:

```
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)# vlan access-map vlan-map-03
switch(config-sync-sp-access-map)# no statistics per-entry
switch(config-sync-sp-access-map)#
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
show running-config switch-profile	Displays the running configuration for a switch profile.
switch-profile	Creates or configures a switch profile.

storm-control level

To set the suppression level for traffic storm control, use the **storm-control level** command. To turn off the suppression mode or revert to the default, use the **no** form of this command.

storm-control {**broadcast** | **multicast** | **unicast**} **level** *percentage*[.*fraction*]

no storm-control {**broadcast** | **multicast** | **unicast**} **level**

Syntax Description

broadcast	Specifies the broadcast traffic.
multicast	Specifies the multicast traffic.
unicast	Specifies the unicast traffic.
level *percentage*	Specifies the percentage of the suppression level. The range is from 0 to 100 percent.
fraction	(Optional) Fraction of the suppression level. The range is from 0 to 99.

Command Default

All packets are passed.

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

Enter the **storm-control level** command to enable traffic storm control on the interface, configure the traffic storm-control level, and apply the traffic storm-control level to all traffic storm-control modes that are enabled on the interface.

The period (.) is required when you enter the fractional-suppression level.

The suppression level is a percentage of the total bandwidth. A threshold value of 100 percent means that no limit is placed on traffic. A threshold value of 0 or 0.0 (fractional) percent means that all specified traffic is blocked on a port.

Use the **show interfaces counters storm-control** command to display the discard count.

Use one of the following methods to turn off suppression for the specified traffic type:

- Set the level to 100 percent for the specified traffic type.
- Use the **no** form of this command.

Examples

This example shows how to enable suppression of broadcast traffic and set the suppression threshold level:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# storm-control broadcast level 30
```

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

This example shows how to disable the suppression mode for multicast traffic:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no storm-control multicast level
switch(config-if)#
```

Related Commands

Command	Description
show interface	Displays the storm-control suppression counters for an interface.
show running-config	Displays the configuration of the interface.

tacacs-server deadtime

To set a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **tacacs-server deadtime** command. To disable the monitoring of the nonresponsive TACACS+ server, use the **no** form of this command.

tacacs-server deadtime *minutes*

no tacacs-server deadtime *minutes*

Syntax Description

time	Time interval in minutes. The range is from 1 to 1440.

Command Default

0 minutes

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

Setting the time interval to zero disables the timer. If the dead-time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead-time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead-time interval for the group is greater than 0 minutes.

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

Examples

This example shows how to configure the dead-time interval and enable periodic monitoring:

```
switch# configure terminal
switch(config)# tacacs-server deadtime 10
switch(config)#
```

This example shows how to revert to the default dead-time interval and disable periodic monitoring:

```
switch# configure terminal
switch(config)# no tacacs-server deadtime 10
switch(config)#
```

Related Commands

Command	Description
deadtime	Sets a dead-time interval for monitoring a nonresponsive RADIUS or TACACS+ server group.
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server information.

tacacs-server directed-request

To allow users to send authentication requests to a specific TACACS+ server when logging in, use the **tacacs-server directed request** command. To revert to the default, use the **no** form of this command.

tacacs-server directed-request

no tacacs-server directed-request

Syntax Description

This command has no arguments or keywords.

Command Default

Sends the authentication request to the configured TACACS+ server groups.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

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

During login, the user can specify the *username@vrfname:hostname*, where *vrfname* is the VRF to use and *hostname* is the name of a configured TACACS+ server. The username is sent to the server name for authentication.

Examples

This example shows how to allow users to send authentication requests to a specific TACACS+ server when logging in:

```
switch# configure terminal
switch(config)# tacacs-server directed-request
switch(config)#
```

This example shows how to disallow users to send authentication requests to a specific TACACS+ server when logging in:

```
switch# configure terminal
switch(config)# no tacacs-server directed-request
switch(config)#
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs-server directed request	Displays a directed request TACACS+ server configuration.

tacacs-server host

To configure TACACS+ server host parameters, use the **tacacs-server host** command. To revert to the defaults, use the **no** form of this command.

tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **7**] *shared-secret*] [**port** *port-number*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds*]

no tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **7**] *shared-secret*] [**port** *port-number*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds*]

Syntax Description

hostname	TACACS+ server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
ipv4-address	TACACS+ server IPv4 address in the *A.B.C.D* format.
ipv6-address	TACACS+ server IPv6 address in the *X:X:X::X* format.
key	(Optional) Configures the TACACS+ server's shared secret key.
0	(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
shared-secret	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.
port *port-number*	(Optional) Configures a TACACS+ server port for authentication. The range is from 1 to 65535.
test	(Optional) Configures parameters to send test packets to the TACACS+ server.
idle-time *time*	(Optional) Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password *password*	(Optional) Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.
username *name*	(Optional) Specifies a user name in the test packets. The username is alphanumeric, case sensitive, and has a maximum of 32 characters.
timeout *seconds*	(Optional) Configures a TACACS+ server timeout period (in seconds) between retransmissions to the TACACS+ server. The range is from 1 to 60 seconds.

Command Default

Idle time: disabled.

Server monitoring: disabled.

Timeout: 1 second.

Test username: test.

Test password: test.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

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

When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

Examples

This example shows how to configure TACACS+ server host parameters:

```
switch# configure terminal
switch(config)# tacacs-server host 192.168.2.3 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs3 key 7 1234
switch(config)# tacacs-server host 192.168.2.3 test idle-time 10
switch(config)# tacacs-server host 192.168.2.3 test username tester
switch(config)# tacacs-server host 192.168.2.3 test password 2B9ka5
switch(config)#
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server information.

tacacs-server key

To configure a global TACACS+ shared secret key, use the **tacacs-server key** command. To remove a configured shared secret, use the **no** form of this command.

tacacs-server key [**0** | **7**] *shared-secret*

no tacacs-server key [**0** | **7**] *shared-secret*

Syntax Description

0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the TACACS+ client and server.
shared-secret	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

You must configure the TACACS+ preshared key to authenticate the switch to the TACACS+ server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all TACACS+ server configurations on the switch. You can override this global key assignment by using the **key** keyword in the **tacacs-server host** command.

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

Examples

This example shows how to display configure TACACS+ server shared keys:

```
switch# configure terminal
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
switch(config)#
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server information.

tacacs-server timeout

To specify the time between retransmissions to the TACACS+ servers, use the **tacacs-server timeout** command. To revert to the default, use the **no** form of this command.

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

Syntax Description

seconds	Seconds between retransmissions to the TACACS+ server. The valid range is 1 to 60 seconds.

Command Default

1 second

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

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

Examples

This example shows how to configure the TACACS+ server timeout value:

```
switch# configure terminal
switch(config)# tacacs-server timeout 3
switch(config)#
```

This example shows how to revert to the default TACACS+ server timeout value:

```
switch# configure terminal
switch(config)# no tacacs-server timeout 3
switch(config)#
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs-server	Displays TACACS+ server information.

telnet6

To create a Telnet session using IPv6 on the Cisco NX-OS switch, use the **telnet6** command.

telnet6 {*ipv6-address* | *hostname*} [*port-number*] [**vrf** {*vrf-name* | **default** | **management**}]

Syntax Description

ipv6-address	IPv6 address of the remote device.
hostname	Hostname of the remote device. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
port-number	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive and can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

Port 23 is the default port. The default VRF is used.

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Telnet server using the **telnet server enable** command.

To create a Telnet session with IPv4 addressing, use the **telnet** command.

Examples

This example shows how to start a Telnet session using an IPv6 address:

```
switch# telnet6 2001:0DB8:0:0:E000::F vrf management
switch#
```

Related Commands

Command	Description
clear line	Clears Telnet sessions.
telnet	Creates a Telnet session using IPv4 addressing.
telnet server enable	Enables the Telnet server.

telnet

To create a Telnet session using IPv4 on a Cisco Nexus 3000 Series switch, use the **telnet** command.

telnet {*ipv4-address* | *hostname*} [*port-number*] [**vrf** {*vrf-name* | **default** | **management**}]

Syntax Description

ipv4-address	IPv4 address of the remote switch.
hostname	Hostname of the remote switch. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
port-number	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive and can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

Port 23 is the default port.

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To create a Telnet session with IPv6 addressing, use the **telnet6** command.

Examples

This example shows how to start a Telnet session using IPv4:

```
switch# telnet 192.168.1.1 vrf management
switch#
```

Related Commands

Command	Description
clear line	Clears Telnet sessions.
telnet server enable	Enables the Telnet server.
telnet6	Creates a Telnet session using IPv6 addressing.

telnet server enable

To enable the Telnet server, use the **telnet server enable** command. To disable the Telnet server, use the **no** form of this command.

telnet server enable

no telnet server enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enable

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to enable the Telnet server:

```
switch(config)# telnet server enable
```

This example shows how to disable the Telnet server:

```
switch(config)# no telnet server enable
```

Related Commands

Command	Description
show telnet server	Displays the Telnet server status.

terminal log-all

To enable logging of all commands, including the **show** commands, to the accounting log, use the **terminal log-all** command. To revert to the default, use the **no** form of this command.

terminal log-all

terminal no log-all

Syntax Description

This command has no arguments or keywords.

Defaults

Does not log the **show** commands.

Command Modes

Any command mode

SupportedUserRoles

network-admin

Command History

Release	Modification
5.0(3)U5(1e)	This command was introduced.

Usage Guidelines

The terminal log setting applies only to the current session.

This command does not require a license.

Examples

This example shows how to enable logging of all commands in the accounting log:

```
switch# terminal log-all
```

This example shows how to disable logging of all commands in the accounting log:

```
switch# terminal no log-all
```

Related Commands

Command	Description
show terminal	Displays the terminal session configuration.

use-vrf

To specify a virtual routing and forwarding (VRF) instance for a RADIUS or TACACS+ server group, use the **use-vrf** command. To remove the VRF instance, use the **no** form of this command.

use-vrf {**vrf-name** | **default** | **management**}

no use-vrf {*vrf-name* | **default** | **management**}

Syntax Description

vrf-name	VRF instance name. The name is case sensitive and can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

None

Command Modes

RADlUS server group configuration mode
TACACS+ server group configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

You can configure only one VRF instance for a server group.

Use the **aaa group server radius** command RADIUS server group configuration mode or the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode.

If the server is not found, use the **radius-server host** command or **tacacs-server host** command to configure the server.

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

Examples

This example shows how to specify a VRF instance for a RADIUS server group:

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)# use-vrf management
switch(config-radius)#
```

This example shows how to specify a VRF instance for a TACACS+ server group:

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# use-vrf management
switch(config-radius)#
```

This example shows how to remove the VRF instance from a TACACS+ server group:

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no use-vrf management
switch(config-radius)#
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature tacacs+	Enables TACACS+.
radius-server host	Configures a RADIUS server.
show radius-server groups	Displays RADIUS server information.
show tacacs-server groups	Displays TACACS+ server information.
tacacs-server host	Configures a TACACS+ server.
vrf	Configures a VRF instance.

username

To create and configure a user account, use the **username** command. To remove a user account, use the **no** form of this command.

username *user-id* [**expire** *date*] [**password** {**0** | **5**} *password*] [**role** *role-name*] [**priv-lvl** *level*]

username *user-id* **sshkey** {*key* | **filename** *filename*}

no username *user-id*

Syntax Description

user-id	User identifier for the user account. The *user-id* argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters. **Note** The Cisco NX-OS software does not allowed the "#" and "@" characters in the *user-id* argument text string.
expire *date*	(Optional) Specifies the expire date for the user account. The format for the *date* argument is YYYY-MM-DD.
password	(Optional) Specifies a password for the account. The default is no password.
0	Specifies that the password that follows should be in clear text. This is the default mode.
5	Specifies that the password that follows should be encrypted.
password	Password for the user (clear text). The password can be a maximum of 64 characters. **Note** Clear text passwords cannot contain dollar signs ($) or spaces anywhere in the password. Also, they cannot include these special characters at the beginning of the password: quotation marks (" or '), vertical bars (|), or right angle brackets (>).
role *role-name*	(Optional) Specifies the role which the user is to be assigned to. Valid values are as follows: • **default-role**—User role • **network-admin**—System configured role • **network-operator**—System configured role • **priv-0**—Privilege role • **priv-1**—Privilege role • **priv-2**—Privilege role • **priv-3**—Privilege role • **priv-4**—Privilege role • **priv-5**—Privilege role • **priv-6**—Privilege role • **priv-7**—Privilege role • **priv-8**—Privilege role • **priv-9**—Privilege role

	• **priv-10**—Privilege role • **priv-11**—Privilege role • **priv-12**—Privilege role • **priv-13**—Privilege role • **priv-14**—Privilege role • **priv-15**—Privilege role • **vdc-admin**—System configured role • **vdc-operator**—System configured role
priv-lvl *level*	(Optional) Specifies the privilege level to assign the user. Valid values are from 0 to 15.
sshkey	(Optional) Specifies an SSH key for the user account.
key	SSH key string.
filename *filename*	Specifies the name of a file that contains the SSH key string.

Command Default

No expiration date, password, or SSH key.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

The switch accepts only strong passwords. The characteristics of a strong password include the following:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

Caution If you do not specify a password for the user account, the user might not be able to log in to the account.

You must enable the cumulative privilege roles for TACACS+ server using the **feature privilege** command to see the **priv-lvl** keyword.

Examples

This example shows how to create a user account with a password:

```
switch# configure terminal
switch(config)# username user1 password Ci5co321
switch(config)#
```

This example shows how to configure the SSH key for a user account:

```
switch# configure terminal
switch(config)# username user1 sshkey file bootflash:key_file
switch(config)#
```

This example shows how to configure the privilege level for a user account:

```
switch# configure terminal
switch(config)# username user1 priv-lvl 15
switch(config)#
```

Related Commands

Command	Description
feature privilege	Enables the cumulative privilege of roles for command authorization on TACACS+ servers.
show privilege	Displays the current privilege level, username, and status of cumulative privilege support for a user.
show user-account	Displays the user account configuration.

vlan access-map

To create a new VLAN access map or to configure an existing VLAN access map, use the **vlan access-map** command. To remove a VLAN access map, use the **no** form of this command.

vlan access-map *map-name*

no vlan access-map *map-name*

Syntax Description

map-name	Name of the VLAN access map that you want to create or configure. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Global configuration mode
Switch profile configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U2(1)	Support for this command was introduced in switch profiles.

Usage Guidelines

Each VLAN access map can include one **match** command and one **action** command.

Examples

This example shows how to create a VLAN access map named vlan-map-01, assign an IPv4 ACL named ip-acl-01 to the map, specify that the switch forwards packets matching the ACL, and enable statistics for traffic matching the map:

```
switch# configure terminal
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
switch(config-access-map)#
```

This example shows how to create a VLAN access map named vlan-map-03 in a switch profile:

```
switch# configure terminal
switch# configure sync
switch(config-sync)# switch-profile s5010
switch(config-sync-sp)# vlan access-map vlan-map-03
switch(config-sync-sp-access-map)#
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan filter	Applies a VLAN access map to one or more VLANs.

vlan filter

To apply a VLAN access map to one or more VLANs, use the **vlan filter** command. To unapply a VLAN access map, use the **no** form of this command.

vlan filter *map-name* **vlan-list** *VLAN-list*

no vlan filter *map-name* [**vlan-list** *VLAN-list*]

Syntax Description

map-name	Name of the VLAN access map that you want to create or configure.
vlan-list *VLAN-list*	Specifies the ID of one or more VLANs whose traffic the VLAN access map filters. Use a hyphen (-) to separate the beginning and ending IDs of a range of VLAN IDs; for example, use 70-100. Use a comma (,) to separate individual VLAN IDs and ranges of VLAN IDs; for example, use 20,70-100,142. **Note** When you use the **no** form of this command, the *VLAN-list* argument is optional. If you omit this argument, the switch removes the access map from all VLANs where the access map is applied.

Command Default

None

Command Modes

Global configuration mode
Switch profile configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U2(1)	Support for this command was introduced in switch profiles.

Usage Guidelines

You can apply a VLAN access map to one or more VLANs.

You can apply only one VLAN access map to a VLAN.

The **no** form of this command enables you to unapply a VLAN access map from all or part of the VLAN list that you specified when you applied the access map. To unapply an access map from all VLANs where it is applied, you can omit the *VLAN-list* argument. To unapply an access map from a subset of the VLANs where it is currently applied, use the *VLAN-list* argument to specify the VLANs where the access map should be removed.

Examples

This example shows how to apply a VLAN access map named vlan-map-01 to VLANs 20 through 45:

```
switch# configure terminal
switch(config)# vlan filter vlan-map-01 20-45
```

```
switch(config)#
```

This example shows how to apply a VLAN access map named vlan-map-03 to VLANs 12 through 20:

```
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)# vlan filter vlan-map-03 12-20
switch(config-sync-sp)#
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show running-config switch-profile	Displays the running configuration for a switch profile.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.

vlan policy deny

To enter VLAN policy configuration mode for a user role, use the **vlan policy deny** command. To revert to the default VLAN policy for a user role, use the **no** form of this command.

vlan policy deny

no vlan policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

All VLANs

Command Modes

User role configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to enter VLAN policy configuration mode for a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)#
```

This example shows how to revert to the default VLAN policy for a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# no vlan policy deny
switch(config-role)#
```

Related Commands

Command	Description
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

vrf policy deny

To configure the deny access to a virtual forwarding and routing instance (VRF) policy for a user role, use the **vrf policy deny** command. To revert to the default VRF policy configuration for a user role, use the **no** form of this command.

vrf policy deny

no vrf policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User role configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to enter VRF policy configuration mode for a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)#
```

This example shows how to revert to the default VRF policy for a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# no vrf policy deny
switch(config-role)#
```

Related Commands

Command	Description
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

vsan policy deny

To configure the deny access to a VSAN policy for a user role, use the **vsan policy deny** command. To revert to the default VSAN policy configuration for a user role, use the **no** form of this command.

vsan policy deny

no vsan policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User role configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.

Usage Guidelines

To permit access to the VSAN policy, use the **permit vsan** command.

Examples

This example shows how to deny access to a VSAN policy for a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# vsan policy deny
switch(config-role-vsan)#
```

This example shows how to revert to the default VSAN policy configuration for a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# vsan policy deny
switch(config-role-vsan)# no vsan policy deny
switch(config-role)#
```

Related Commands

Command	Description
permit vsan	Configures permit access to a VSAN policy for a user.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.