



Send comments to nexus5k-docfeedback@cisco.com



Cisco Nexus 5000 Series NX-OS Security Command Reference

Cisco NX-OS Releases 4.x, 5.x

First Published: October 2008

Last Modified: February 2013

Americas Headquarters

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

Text Part Number: OL-25833-01

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

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

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

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

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

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

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

Cisco Nexus 5000 Series NX-OS Security Command Reference
© 2008-2012 Cisco Systems, Inc. All rights reserved.

Send comments to nexus5k-docfeedback@cisco.com



CONTENTS

Preface **xi**

Audience **xi**

Supported Switches **xi**

 Cisco Nexus 5000 Platform Switches **xi**

 Cisco Nexus 5500 Platform Switches **xii**

Organization **xii**

Document Conventions **xiii**

Related Documentation **xiv**

 Release Notes **xiv**

 Configuration Guides **xiv**

 Maintain and Operate Guides **xv**

 Installation and Upgrade Guides **xv**

 Licensing Guide **xv**

 Command References **xv**

 Technical References **xv**

 Error and System Messages **xvi**

 Troubleshooting Guide **xvi**

Obtaining Documentation and Submitting a Service Request **xvi**

xvi

New and Changed Information **xvii**

New and Changed Information for Cisco NX-OS Releases **xvii**

 New and Changed Information for Cisco NX-OS Release 5.2(1)N1(1) **xvii**

 New and Changed Information for Cisco NX-OS Release 5.1(3)N1(1) **xviii**

 New and Changed Information for Cisco NX-OS Release 5.0(3)N2(1) **xviii**

 New and Changed Information for Cisco NX-OS Release 5.0(3)N1(1) **xviii**

 New and Changed Information for Cisco NX-OS Release 5.0(2)N2(1) **xix**

 New and Changed Information for Cisco NX-OS Release 5.0(2)N1(1) **xx**

A Commands **SEC-1**

 aaa accounting default **SEC-2**

 aaa authentication login console **SEC-3**

 aaa authentication login default **SEC-5**

Send comments to nexus5k-docfeedback@cisco.com

[aaa authentication login error-enable](#) **SEC-7**
[aaa authentication login mschap enable](#) **SEC-8**
[aaa authorization commands default](#) **SEC-9**
[aaa authorization config-commands default](#) **SEC-11**
[aaa authorization ssh-certificate](#) **SEC-13**
[aaa authorization ssh-publickey](#) **SEC-15**
[aaa group server radius](#) **SEC-17**
[aaa user default-role](#) **SEC-18**
[access-class](#) **SEC-19**
[action](#) **SEC-21**

C Commands **SEC-23**

[checkpoint](#) **SEC-24**
[clear access-list counters](#) **SEC-26**
[clear accounting log](#) **SEC-27**
[clear checkpoint database](#) **SEC-28**
[clear ip arp](#) **SEC-29**
[clear ip arp inspection log](#) **SEC-30**
[clear ip arp inspection statistics vlan](#) **SEC-31**
[clear ip dhcp snooping binding](#) **SEC-32**
[clear ip dhcp snooping statistics](#) **SEC-34**

D Commands **SEC-35**

[deadtime](#) **SEC-36**
[deny icmp \(IPv4\)](#) **SEC-38**
[deny igmp \(IPv4\)](#) **SEC-44**
[deny ip \(IPv4\)](#) **SEC-48**
[deny tcp \(IPv4\)](#) **SEC-52**
[deny udp \(IPv4\)](#) **SEC-60**
[deny icmp \(IPv6\)](#) **SEC-66**
[deny ipv6 \(IPv6\)](#) **SEC-70**
[deny sctp \(IPv6\)](#) **SEC-74**
[deny tcp \(IPv6\)](#) **SEC-79**
[deny udp \(IPv6\)](#) **SEC-85**
[deny \(MAC\)](#) **SEC-90**
[description \(user role\)](#) **SEC-93**

Send comments to nexus5k-docfeedback@cisco.com

E Commands SEC-95

enable SEC-96

enable secret SEC-97

F Commands SEC-99

feature (user role feature group) SEC-100

feature dhcp SEC-101

feature http-server SEC-103

feature port-security SEC-105

feature privilege SEC-107

feature tacacs+ SEC-108

I Commands SEC-109

interface policy deny SEC-110

ip access-class SEC-111

ip access-group SEC-113

ip access-list SEC-115

ip arp event-history errors SEC-117

ip arp inspection log-buffer SEC-118

ip arp inspection validate SEC-119

ip arp inspection vlan SEC-121

ip arp inspection trust SEC-123

ip dhcp packet strict-validation SEC-124

ip dhcp snooping SEC-125

ip dhcp snooping information option SEC-126

ip dhcp snooping trust SEC-127

ip dhcp snooping verify mac-address SEC-128

ip dhcp snooping vlan SEC-129

ip port access-group SEC-130

ip source binding SEC-132

ip verify source dhcp-snooping-vlan SEC-134

ip verify unicast source reachable-via SEC-136

ipv6 access-class SEC-138

ipv6 access-list SEC-140

ipv6 port traffic-filter SEC-141

ipv6 traffic-filter SEC-143

Send comments to nexus5k-docfeedback@cisco.com

M Commands SEC-145

mac access-list SEC-146
mac port access-group SEC-148
match SEC-150

P Commands SEC-153

permit icmp (IPv4) SEC-154
permit igmp (IPv4) SEC-160
permit ip (IPv4) SEC-164
permit tcp (IPv4) SEC-168
permit udp (IPv4) SEC-177
permit icmp (IPv6) SEC-183
permit ipv6 (IPv6) SEC-188
permit sctp (IPv6) SEC-192
permit tcp (IPv6) SEC-197
permit udp (IPv6) SEC-203
permit (MAC) SEC-209
permit interface SEC-212
permit vlan SEC-214
permit vrf SEC-216
permit vsan SEC-217

R Commands SEC-219

radius-server deadtime SEC-220
radius-server directed-request SEC-221
radius-server host SEC-222
radius-server key SEC-224
radius-server retransmit SEC-225
radius-server timeout SEC-226
remark SEC-227
resequence SEC-229
role feature-group name SEC-231
role name SEC-232
rollback running-config SEC-234
rule SEC-236

Send comments to nexus5k-docfeedback@cisco.com

S Commands SEC-239

server SEC-240
ssh SEC-242
ssh6 SEC-243
ssh key SEC-244
ssh login-attempts SEC-246
ssh server enable SEC-247
storm-control level SEC-248

Show Commands SEC-251

show aaa accounting SEC-252
show aaa authentication SEC-253
show aaa authorization SEC-254
show aaa groups SEC-255
show aaa user SEC-256
show access-lists SEC-257
show accounting log SEC-259
show arp access-lists SEC-261
show checkpoint SEC-262
show checkpoint summary SEC-265
show checkpoint system SEC-267
show checkpoint user SEC-268
show diff rollback-patch checkpoint SEC-270
show diff rollback-patch file SEC-272
show diff rollback-patch running-config SEC-274
show diff rollback-patch startup-config SEC-277
show http-server SEC-280
show ip access-lists SEC-281
show ip arp SEC-283
show ip arp inspection SEC-285
show ip arp inspection interfaces SEC-286
show ip arp inspection log SEC-287
show ip arp inspection statistics SEC-288
show ip arp inspection vlan SEC-289
show ip arp sync-entries SEC-290
show ip dhcp snooping SEC-291

Send comments to nexus5k-docfeedback@cisco.com

[show ip dhcp snooping binding](#) **SEC-292**
[show ip dhcp snooping statistics](#) **SEC-294**
[show ipv6 access-lists](#) **SEC-295**
[show ip verify source](#) **SEC-297**
[show mac access-lists](#) **SEC-299**
[show privilege](#) **SEC-300**
[show radius-server](#) **SEC-301**
[show role](#) **SEC-304**
[show role feature](#) **SEC-308**
[show role feature-group](#) **SEC-311**
[show rollback log](#) **SEC-312**
[show running-config aaa](#) **SEC-314**
[show running-config aclmgr](#) **SEC-315**
[show running-config arp](#) **SEC-317**
[show running-config dhcp](#) **SEC-319**
[show running-config radius](#) **SEC-322**
[show running-config security](#) **SEC-323**
[show ssh key](#) **SEC-325**
[show ssh server](#) **SEC-326**
[show startup-config aaa](#) **SEC-327**
[show startup-config aclmgr](#) **SEC-328**
[show startup-config arp](#) **SEC-330**
[show startup-config dhcp](#) **SEC-331**
[show startup-config radius](#) **SEC-333**
[show startup-config security](#) **SEC-334**
[show tacacs-server](#) **SEC-335**
[show telnet server](#) **SEC-337**
[show user-account](#) **SEC-338**
[show users](#) **SEC-339**
[show vlan access-list](#) **SEC-340**
[show vlan access-map](#) **SEC-341**
[show vlan filter](#) **SEC-342**

T Commands **SEC-343**

[tacacs-server deadline](#) **SEC-344**
[tacacs-server directed-request](#) **SEC-345**

Send comments to nexus5k-docfeedback@cisco.com

[tacacs-server host](#) **SEC-346**
[tacacs-server key](#) **SEC-348**
[tacacs-server timeout](#) **SEC-349**
[telnet](#) **SEC-350**
[telnet server enable](#) **SEC-351**
[telnet6](#) **SEC-352**

U Commands **SEC-353**

[use-vrf](#) **SEC-354**
[username](#) **SEC-356**

V Commands **SEC-359**

[vlan access-map](#) **SEC-360**
[vlan filter](#) **SEC-361**
[vlan policy deny](#) **SEC-363**
[vrf policy deny](#) **SEC-364**
[vsan policy deny](#) **SEC-365**

Send comments to nexus5k-docfeedback@cisco.com



Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 5000 Series NX-OS Security Command Reference*. It also provides information on how to obtain related documentation.

This preface includes the following sections:

- [Audience, page xi](#)
- [Supported Switches, page xi](#)
- [Organization, page xii](#)
- [Document Conventions, page xiii](#)
- [Related Documentation, page xiv](#)
- [Obtaining Documentation and Submitting a Service Request, page xvi](#)

Audience

This publication is for experienced users who configure and maintain Cisco NX-OS devices.

Supported Switches

This section includes the following topics:

- [Cisco Nexus 5000 Platform Switches, page xi](#)
- [Cisco Nexus 5500 Platform Switches, page xii](#)

Cisco Nexus 5000 Platform Switches

[Table 1](#) lists the Cisco switches supported in the Cisco Nexus 5000 Platform.



Note

For more information on these switches, see the *Cisco Nexus 5500 Platform and Cisco Nexus 5000 Platform Hardware Installation Guide* available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

Send comments to nexus5k-docfeedback@cisco.com

Table 1 Supported Cisco Nexus 5000 Platform Switches

Switch	Description
Cisco Nexus 5010 Switch	The Cisco Nexus 5010 is a 1 rack unit (RU) switch. It delivers 500 Gbps of wire-speed switching capacity designed for traditional, virtualized, unified, and high-performance computing (HPC) environments.
Cisco Nexus 5020 Switch	The Cisco Nexus 5020 is a 2 rack unit (RU) switch. It delivers 1+ Tbps of wire-speed switching capacity designed for traditional, virtualized, unified, and HPC environments.



Note

The Cisco Nexus 5000 Platform switches only supports Internet Group Management Protocol (IGMP) snooping. IGMP, Protocol Independent Multicast (PIM), and Multicast Source Discovery Protocol (MSDP) are not supported on the Cisco Nexus 5000 Platform switches.

Cisco Nexus 5500 Platform Switches

Table 2 lists the Cisco switches supported in the Cisco Nexus 5500 Platform.



Note

For more information on these switches, see the *Cisco Nexus 5500 Platform and Cisco Nexus 5000 Platform Hardware Installation Guide* available at the following URL:
http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

Table 2 Supported Cisco Nexus 5500 Platform Switches

Switch	Description
Cisco Nexus 5548P Switch	The Cisco Nexus 5548P switch is the first switch in the Cisco Nexus 5500 Platform. It is a one-rack-unit (1 RU), 10-Gigabit Ethernet and Fibre Channel over Ethernet (FCoE) switch that offers up to 960-Gbps throughput and up to 48 ports.
Cisco Nexus 5596P Switch	The Cisco Nexus 5596P switch is a top-of-rack, 10-Gigabit Ethernet and FCoE switch offering up to 1920-Gigabit throughput and up to 96 ports.

Organization

This document is organized as follows:

Send comments to nexus5k-docfeedback@cisco.com

Chapter Title	Description
New and Changed Information	Describes the new and changed information for the new Cisco NX-OS software releases.
A Commands	Describes the Cisco NX-OS security commands that begin with B.
C Commands	Describes the Cisco NX-OS security commands that begin with C.
D Commands	Describes the Cisco NX-OS security commands that begin with D.
E Commands	Describes the Cisco NX-OS security commands that begin with E.
F Commands	Describes the Cisco NX-OS security commands that begin with F.
I Commands	Describes the Cisco NX-OS security commands that begin with I.
M Commands	Describes the Cisco NX-OS security commands that begin with M.
P Commands	Describes the Cisco NX-OS security commands that begin with P.
R Commands	Describes the Cisco NX-OS security commands that begin with R.
S Commands	Describes the Cisco NX-OS security commands that begin with S.
Show Commands	Describes the Cisco NX-OS security show commands.
T Commands	Describes the Cisco NX-OS security commands that begin with T.
U Commands	Describes the Cisco NX-OS security commands that begin with U.
V Commands	Describes the Cisco NX-OS security commands that begin with V.

Document Conventions

Command descriptions use these conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
<i>italic font</i>	Arguments for which you supply values are in italics.
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[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 you must enter is in boldface screen font.
<i>italic screen font</i>	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Send comments to nexus5k-docfeedback@cisco.com

[]	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 Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extender is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

The following are related Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender documents:

Release Notes

Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes

Cisco Nexus 5000 Series Switch Release Notes

Configuration Guides

Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 5.0(2)N1(1)

Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 4.2(1)N1(1) and Release 4.2(1)N2(1)

Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide

Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide

Cisco Nexus 5000 Series NX-OS Multicast Routing Configuration Guide

Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide

Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide

Cisco Nexus 5000 Series NX-OS Security Configuration Guide

Cisco Nexus 5000 Series NX-OS System Management Configuration Guide

Cisco Nexus 5000 Series NX-OS Unicast Routing Configuration Guide

Cisco Nexus 5000 Series Switch NX-OS Software Configuration Guide

Send comments to nexus5k-docfeedback@cisco.com

Cisco Nexus 5000 Series Fabric Manager Configuration Guide, Release 3.4(1a)

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

Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide

Maintain and Operate Guides

Cisco Nexus 5000 Series NX-OS Operations Guide

Installation and Upgrade Guides

Cisco Nexus 5000 Series and Cisco Nexus 5500 Platform Hardware Installation Guide

Cisco Nexus 2000 Series Hardware Installation Guide

Cisco Nexus 5000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.2(1)N1(1)

Regulatory Compliance and Safety Information for the Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders

Licensing Guide

Cisco NX-OS Licensing Guide

Command References

Cisco Nexus 5000 Series NX-OS FabricPath Command Reference

Cisco Nexus 5000 Series NX-OS Fabric Extender Command Reference

Cisco Nexus 5000 Series NX-OS Fibre Channel Command Reference

Cisco Nexus 5000 Series NX-OS Fundamentals Command Reference

Cisco Nexus 5000 Series NX-OS Layer 2 Interfaces Command Reference

Cisco Nexus 5000 Series NX-OS Multicast Routing Command Reference

Cisco Nexus 5000 Series NX-OS QoS Command Reference

Cisco Nexus 5000 Series NX-OS Security Command Reference

Cisco Nexus 5000 Series NX-OS System Management Command Reference

Cisco Nexus 5000 Series NX-OS TrustSec Command Reference

Cisco Nexus 5000 Series NX-OS Unicast Routing Command Reference

Cisco Nexus 5000 Series NX-OS vPC Command Reference

Technical References

Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender MIBs Reference

Send comments to nexus5k-docfeedback@cisco.com

Error and System Messages

Cisco NX-OS System Messages Reference

Troubleshooting Guide

Cisco Nexus 5000 Troubleshooting Guide

Obtaining Documentation and Submitting a Service Request

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

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

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

Send comments to nexus5k-docfeedback@cisco.com



New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 5000 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/ps9670/prod_command_reference_list.html

To check for additional information about this Cisco NX-OS Release, see the *Cisco Nexus 5000 Series Switch Release Notes* available at the following Cisco website:

http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

New and Changed Information for Cisco NX-OS Releases

This section includes the following topics:

- [New and Changed Information for Cisco NX-OS Release 5.2\(1\)N1\(1\)](#), page xvii
- [New and Changed Information for Cisco NX-OS Release 5.1\(3\)N1\(1\)](#), page xviii
- [New and Changed Information for Cisco NX-OS Release 5.0\(3\)N2\(1\)](#), page xviii
- [New and Changed Information for Cisco NX-OS Release 5.0\(3\)N1\(1\)](#), page xviii
- [New and Changed Information for Cisco NX-OS Release 5.0\(2\)N2\(1\)](#), page xix
- [New and Changed Information for Cisco NX-OS Release 5.0\(2\)N1\(1\)](#), page xx

New and Changed Information for Cisco NX-OS Release 5.2(1)N1(1)

[Table 2](#) summarizes the new and changed features for Cisco NX-OS Release 5.2(1)N1(1) and tells you where they are documented.

Table 1 *New and Changed Information for Release 5.2(1)N1(1)*

Feature	Description	Where Documented
IPv6	Added support for IPv6.	ipv6 traffic-filter resequence

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

New and Changed Information for Cisco NX-OS Release 5.1(3)N1(1)

Table 2 summarizes the new and changed features for Cisco NX-OS Release 5.1(3)N1(1) and tells you where they are documented.

Table 2 *New and Changed Information for Release 5.1(3)N1(1)*

Feature	Description	Where Documented
IP ARP synchronization	This command was updated.	show ip arp sync-entries
Support for virtual Ethernet interfaces	The following commands were updated to extend support for virtual Ethernet interface configurations: <ul style="list-style-type: none"> ip port access-group ipv6 port traffic-filter mac port access-group show ip arp 	ip port access-group ipv6 port traffic-filter mac port access-group show ip arp

New and Changed Information for Cisco NX-OS Release 5.0(3)N2(1)

There are no new and changed features for Cisco NX-OS Release 5.0(3)N2(1).

New and Changed Information for Cisco NX-OS Release 5.0(3)N1(1)

Table 3 summarizes the new and changed features for Cisco NX-OS Release 5.0(3)N1(1) and tells you where they are documented.

Table 3 *New and Changed Information for Release 5.0(3)N1(1)*

Feature	Description	Changed in Release	Where Documented
IP access group	Added the ip access-group command to apply an IPv4 access control list (ACL) to an interface as a router ACL.	5.0(3)N1(1)	ip access-group
IP Source Guard	This feature was introduced. The following IP Source Guard commands for Layer 2 Ethernet interfaces were introduced: <ul style="list-style-type: none"> ip verify source dhcp-snooping-vlan show ip verify source 	5.0(3)N1(1)	ip verify source dhcp-snooping-vlan show ip verify source

Send comments to nexus5k-docfeedback@cisco.com

Table 3 ***New and Changed Information for Release 5.0(3)N1(1) (continued)***

Feature	Description	Changed in Release	Where Documented
Dynamic ARP Inspection (DAI)	<p>This feature was introduced.</p> <p>Added the following commands to configure dynamic Address Resolution Protocol (ARP) inspection (DAI) on a Cisco NX-OS switch:</p> <ul style="list-style-type: none"> • ip arp inspection log-buffer • ip arp inspection validate • ip arp inspection vlan 	5.0(3)N1(1)	clear ip arp inspection log clear ip arp inspection statistics vlan ip arp inspection log-buffer ip arp inspection validate ip arp inspection vlan show ip arp inspection show ip arp inspection interfaces show ip arp inspection log show ip arp inspection statistics
Unicast RPF	<p>Added the ip verify unicast source reachable-via command to configure Unicast Reverse Path Forwarding (Unicast RPF) on an interface.</p>	5.0(3)N1(1)	ip verify unicast source reachable-via

New and Changed Information for Cisco NX-OS Release 5.0(2)N2(1)

[Table 4](#) summarizes the new and changed features for Cisco NX-OS Release 5.0(2)N2(1) and tells you where they are documented.

Send comments to nexus5k-docfeedback@cisco.com

Table 4 *New and Changed Information for Release 5.0(2)N2(1)*

Feature	Description	Changed in Release	Where Documented
Release 5.0(2)N2(1)			
DHCP Snooping	You can configure DHCP snooping on switches and VLANs.	5.0(2)N2(1)	clear ip dhcp snooping binding clear ip dhcp snooping statistics feature dhcp ip dhcp packet strict-validation ip dhcp snooping 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

New and Changed Information for Cisco NX-OS Release 5.0(2)N1(1)

[Table 5](#) summarizes the new and changed features for Cisco NX-OS Release 5.0(2)N1(1) and tells you where they are documented.

Table 5 *New and Changed Information for Release 5.0(2)N1(1)*

Feature	Description	Changed in Release	Where Documented
Release 5.0(2)N1(1)			
Support for HTTP server	You can enable HTTP or Hypertext Transfer Protocol Secure (HTTPS) on a switch.	5.0(2)N1(1)	feature http-server
Privilege level	<p>You can enable the cumulative privilege of roles for command authorization on RADIUS and TACACS+ servers.</p> <p>You can also enable a user to move to a higher privilege level, or set a password for a specific privilege level.</p>	5.0(2)N1(1)	enable enable secret feature privilege role name rule show privilege

Send comments to nexus5k-docfeedback@cisco.com

Table 5 ***New and Changed Information for Release 5.0(2)N1(1) (continued)***

Feature	Description	Changed in Release	Where Documented
ACLs on VTY	You can configure an access class to restrict incoming or outgoing traffic on a virtual terminal line (VTY).	5.0(2)N1(1)	access-class ip access-class ip access-list show running-config aclmgr show startup-config aclmgr
Checkpoint and rollback	You can take a snapshot of the current running configuration or roll back to a specified checkpoint to restore the active configuration of the system.	5.0(2)N1(1)	checkpoint clear checkpoint database rollback running-config show checkpoint show checkpoint summary show checkpoint system show checkpoint user show diff rollback-patch checkpoint show diff rollback-patch file show diff rollback-patch running-config show diff rollback-patch startup-config show rollback log
SSH	You can set the number of login attempts that a user can try before being disconnected.	5.0(2)N1(1)	ssh login-attempts

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com



A Commands

This chapter describes the Cisco NX-OS security commands that begin with A.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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.
<i>group-list</i>	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
4.0(0)N1(1a)	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(config)# aaa accounting default group
```

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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.
<i>group-list</i>	Space-separated list of RADIUS or TACACS+ server groups. The list can include the following: <ul style="list-style-type: none">• 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
4.0(0)N1(1a)	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(config)# aaa authentication login console group radius
```

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

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

Send comments to nexus5k-docfeedback@cisco.com

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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.
<i>group-list</i>	Space-separated list of RADIUS or TACACS+ server groups that can include the following: <ul style="list-style-type: none">• 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
4.0(0)N1(1a)	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(config)# aaa authentication login default group radius
```

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

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

Send comments to nexus5k-docfeedback@cisco.com

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.

Send comments to nexus5k-docfeedback@cisco.com

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
4.0(0)N1(1a)	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(config)# aaa authentication login error-enable
```

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

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

Related Commands

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

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to enable MS-CHAP authentication:

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

This example shows how to disable MS-CHAP authentication:

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

Related Commands

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

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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.
<i>group-list</i>	List of server groups. The list can include the following: <ul style="list-style-type: none">• 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
4.2(1)N1(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:

Send comments to nexus5k-docfeedback@cisco.com

```
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(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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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.
<i>group-list</i>	List of server groups. The list can include the following: <ul style="list-style-type: none">• 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
4.2(1)N1(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.

Send comments to nexus5k-docfeedback@cisco.com

Examples

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

```
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(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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

aaa authorization ssh-certificate

To configure the default authentication, authorization, and accounting (AAA) authorization method for TACACS+ servers, use the **aaa authorization ssh-certificate** command. To disable this configuration, use the **no** form of this command.

aaa authorization ssh-certificate default {group *group-list* | local}

no aaa authorization ssh-certificate default {group *group-list* | local}

Syntax Description

group	Specifies to use a server group for authorization.
<i>group-list</i>	Space-separated list of server groups. The list can include the following: <ul style="list-style-type: none">• tacacs+ for all configured TACACS+ servers.• Any configured TACACS+ server group name. The server group name can be a maximum of 127 characters.
local	Specifies to use the local database for authentication.

Command Default

local

Command Modes

Global configuration mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

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

The **group tacacs+** and **group *group-list*** methods refer to a set of previously defined TACACS+ and LDAP 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 is used only if all the configured server groups fail to respond and you have configured **local** as the fallback method.

If you specify the **group** method or **local** method and it fails, the authorization can fail. If you have not configured a fallback method after the TACACS+ or LDAP server group method, authorization fails if all server groups fail to respond.

This command does not require a license.

Send comments to nexus5k-docfeedback@cisco.com

Examples

This example shows how to configure the local database with certificate authentication as the default AAA authorization method:

```
switch# configure terminal
switch(config)# aaa authorization ssh-certificate default local
switch(config)#
```

Related Commands

Command	Description
aaa authorization ssh-publickey	Configures local authorization with the SSH public key as the default AAA authorization method.
feature tacacs+	Enables the TACACS+ feature.
show aaa authorization	Displays the AAA authorization configuration.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

aaa authorization ssh-publickey

To configure local authorization with the Secure Shell (SSH) public key as the default AAA authorization method for TACACS+ servers, use the **aaa authorization ssh-publickey** command. To revert to the default, use the **no** form of this command.

```
aaa authorization ssh-publickey default {group group-list | local}
```

```
no aaa authorization ssh-publickey default {group group-list | local}
```

Syntax Description

group	Specifies to use a server group for authorization.
<i>group-list</i>	Space-separated list of server groups. The server group name can be a maximum of 127 characters.
local	Specifies to use the local database for authentication.

Command Default

local

Command Modes

Global configuration mode

Command History

Release	Modification
5.1(3)N1(1)	This command was introduced.

Usage Guidelines

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 is used only if all the configured server groups fail to respond and you have configured **local** as the fallback method.

If you specify the **group** method or **local** method and it fails, the authorization can fail. If you have not configured a fallback method after the server group method, authorization fails if all server groups fail to respond.

This command does not require a license.

Examples

This example shows how to configure local authorization with the SSH public key as the default AAA authorization method:

```
switch# configure terminal
switch(config)# aaa authorization ssh-publickey default local
switch(config)#
```

Send comments to nexus5k-docfeedback@cisco.com

Related Commands	Command	Description
	aaa authorization ssh-certificate	Configures local authorization with certificate authentication as the default AAA authorization method.
	show aaa authorization	Displays the AAA authorization configuration.

Send comments to nexus5k-docfeedback@cisco.com

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	<i>group-name</i>	RADIUS server group name.
--------------------	-------------------	---------------------------

Command Default	None
-----------------	------

Command Modes	Global configuration mode
---------------	---------------------------

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

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

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

This example shows how to delete a RADIUS server group:

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

Related Commands	Command	Description
	show aaa groups	Displays server group information.

Send comments to nexus5k-docfeedback@cisco.com

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
4.0(0)N1(1a)	This command was introduced.

Examples

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

```
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(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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

access-class

To restrict incoming and outgoing connections between a particular VTY (into a Cisco Nexus 5000 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

<i>access-list-name</i>	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 5000 Series switch and the addresses in the access list.
out	Specifies that outgoing connections be restricted between a particular Cisco Nexus 5000 Series switch and the addresses in the access list.

Command Default

None

Command Modes

Line configuration mode

Command History

Release	Modification
5.0(2)N1(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(config)# line vty
switch(config-line)# no access-class ozi2 in
switch(config-line)#
```

Send comments to nexus5k-docfeedback@cisco.com

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.

Send comments to nexus5k-docfeedback@cisco.com

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 mode	
Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.
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	<p>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:</p> <pre>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</pre>	
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.

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com



C Commands

This chapter describes the Cisco NX-OS security commands that begin with C.

Send comments to nexus5k-docfeedback@cisco.com

checkpoint

To take a snapshot of the current running configuration and store the snapshot in the file system in an ASCII format, use the **checkpoint** command.

checkpoint [*checkpoint-name* [**description** *descp-text* [...**description** *descp-text*]] | **description** *descp-text* | **file** { **bootflash:** | **volatile:** } [*//server*][*/directory/*][*filename*]]

no checkpoint [*checkpoint-name* | **description** *descp-text* | **file** { **bootflash:** | **volatile:** } [*//server*][*/directory/*][*filename*]]

Syntax Description

<i>checkpoint-name</i>	(Optional) Checkpoint name. The name can be a maximum of 32 characters.
description <i>descp-text</i>	(Optional) Specifies a description for the given checkpoint. The text can be a maximum of 80 characters and can contain spaces.
file	(Optional) Specifies that a file be created to store the configuration rollback checkpoint.
bootflash:	Specifies the bootflash local writable storage file system.
volatile:	Specifies the volatile local writable storage file system.
<i>//server</i>	(Optional) Name of the server. Valid values are <i>///</i> , <i>//module-1/</i> , <i>//sup-1/</i> , <i>//sup-active/</i> , or <i>//sup-local/</i> . The double slash (<i>//</i>) is required.
<i>/directory/</i>	(Optional) Name of a directory. The directory name is case sensitive.
<i>filename</i>	(Optional) Name of the checkpoint configuration file. The filename is case sensitive.



Note

There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

Automatically generates checkpoint name (*user-checkpoint-number*).

Command Modes

EXEC mode

Command History

Release	Modification
5.0(2)N1(1)	This command was introduced.

Usage Guidelines

Checkpoints are local to a switch. When you create a checkpoint, a snapshot of the current running configuration is stored in a checkpoint file. If you do not provide a checkpoint name, Cisco NX-OS sets the checkpoint name to **user-checkpoint-number**, where the *number* is from 1 to 10.

If Fibre Channel over Ethernet (FCoE) is enabled on the switch, you cannot restore the active configuration to the checkpoint state. The following error message appears when you create a checkpoint on a FCoE-enabled switch:

Send comments to nexus5k-docfeedback@cisco.com

```
switch# checkpoint chkpoint-1
ERROR: ascii-cfg: FCOE is enabled. Disbaling rollback module (err_id 0x405F004C)
switch#
```

On a switch that has FCoE disabled, you see the following message when you create the checkpoint:

```
switch# checkpoint chkpoint-1
...Done
switch#
```

You can create up to ten checkpoints of your configuration per switch. When the number of checkpoints reaches the maximum limit, the oldest entry is removed.

You cannot apply the checkpoint file of one switch into another switch. You cannot start a checkpoint filename with the word *system*.

The checkpoint files are stored as text files that you cannot directly access or modify. When a checkpoint is cleared from the system, the associated checkpoint configuration file is deleted.

Examples

This example shows how to create a checkpoint:

```
switch# checkpoint
...
user-checkpoint-4 created Successfully

Done
switch#
```

This example shows how to create a checkpoint, named chkpt-1, and define its purpose:

```
switch# checkpoint chkpt-1 description Checkpoint to save current configuration, Sep 9 10:02 A.M.
switch#
```

This example shows how to create a checkpoint configuration file named chkpt_configSep9-1.txt in the bootflash storage system:

```
switch# checkpoint file bootflash:///chkpt_configSep9-1.txt
switch#
```

This example shows how to delete a checkpoint named chkpt-1:

```
switch# no checkpoint chkpt-1
switch#
```

Related Commands

Command	Description
clear checkpoint	Clears the checkpoints on the switch.
rollback	Rolls back the switch to any of the saved checkpoints.
show checkpoint all	Displays all checkpoints configured in the switch.
show checkpoint summary	Displays a summary of all checkpoints configured in the switch.
show checkpoint summary user	Displays all checkpoints created by an user.
show checkpoint system	Displays all checkpoints that were automatically created in the system.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	<i>access-list-name</i>	(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
	4.0(0)N1(1a)	This command was introduced.

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

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

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

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

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.

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	This command was introduced.

Examples	<p>This example shows how to clear the accounting log:</p> <pre>switch# clear accounting log</pre>
-----------------	---

Related Commands	Command	Description
	show accounting log	Displays the accounting log contents.

Send comments to nexus5k-docfeedback@cisco.com

clear checkpoint database

To clear the checkpoints configured on the switch, use the **clear checkpoint database** command.

clear checkpoint database [system | user]

Syntax Description	system	Clears the configuration rollback checkpoint database for system checkpoints.
	user	Clears the configuration rollback checkpoint database for user checkpoints.

Command Default	None
-----------------	------

Command Modes	EXEC mode
---------------	-----------

Command History	Release	Modification
	5.0(2)N1(1)	This command was introduced.

Examples This example shows how to clear the configured checkpoints:

```
switch# clear checkpoint database
.Done
switch#
```

Related Commands	Command	Modification
	checkpoint	Creates a checkpoint.
	show checkpoint	Displays all configured checkpoints.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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 <i>vlan-id</i>	(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.
	<i>vrf-name</i>	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
	4.2(1)N1(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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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)N1(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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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 <i>vlan-list</i>	Specifies the VLANs whose DAI statistics this command clears. The <i>vlan-list</i> 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)N1(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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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 <i>vlan-id</i>		(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 <i>mac-address</i>		(Optional) Specifies the MAC address of the binding database entry to be cleared. Enter the <i>mac-address</i> argument in dotted hexadecimal format.
ip <i>ip-address</i>		(Optional) Specifies the IPv4 address of the binding database entry to be cleared. Enter the <i>ip-address</i> argument in dotted decimal format.
interface		(Optional) Specifies the Ethernet or EtherChannel interface.
ethernet <i>slot/port</i>		(Optional) Specifies the Ethernet interface of the binding database entry to be cleared.
port-channel <i>channel-number</i>		(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(2)N2(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#
```

Send comments to nexus5k-docfeedback@cisco.com

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, including the IP Source Guard configuration.

Send comments to nexus5k-docfeedback@cisco.com

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(2)N2(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, including the IP Source Guard configuration.

Send comments to nexus5k-docfeedback@cisco.com



D Commands

This chapter describes the Cisco NX-OS security commands that begin with D.

Send comments to nexus5k-docfeedback@cisco.com

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	<i>minutes</i>	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
	4.0(0)N1(1a)	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(config)# aaa group server radius RadServer
switch(config-radius)# deadtime 2
```

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

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

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

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

Related Commands	Command	Description
	aaa group server	Configures AAA server groups.
	feature tacacs+	Enables TACACS+.
	radius-server host	Configures a RADIUS server.

Send comments to nexus5k-docfeedback@cisco.com

Command	Description
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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

deny icmp (IPv4)

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

```
[sequence-number] deny icmp source destination [icmp-message | dscp dscp] log | precedence
precedence | fragments]
```

```
no deny icmp source destination [icmp-message | dscp dscp | log | precedence precedence |
fragments]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.
<i>icmp-message</i>	(Optional) 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 the “ICMP Message Types” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(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 <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 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)
fragments	<p>(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.</p>

Send comments to nexus5k-docfeedback@cisco.com

log	<p>(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information:</p> <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable
precedence <i>precedence</i>	<p>(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the <i>precedence</i> argument. The <i>precedence</i> argument can be a number or a keyword as follows:</p> <ul style="list-style-type: none"> • 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)

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

Command History

Release	Modification
5.2(1)N1(1)	Added ACL logging capability.
4.0(0)N1(1a)	This command was introduced.

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:

Send comments to nexus5k-docfeedback@cisco.com

- 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 icmp 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 icmp 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

Send comments to nexus5k-docfeedback@cisco.com

- **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

Examples

This example shows how to configure an IPv4 ACL named `acl-lab-01` with rules that deny all ICMP 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(config)# ip access-list acl-lab-01
switch(config-acl)# deny icmp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny icmp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit ip any any
```

Send comments to nexus5k-docfeedback@cisco.com

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

deny igmp (IPv4)

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

[sequence-number] **deny igmp** *source destination [igmp-message | dscp dscp | precedence precedence | fragments | log]*

no deny igmp *source destination [igmp-message | dscp dscp | precedence precedence | fragments | log]*

no *sequence-number*

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.
<i>igmp-message</i>	(Optional) Rule that matches only packets of the specified IGMP message type. The <i>igmp-message</i> argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords: <ul style="list-style-type: none"> • dvmrp—Distance Vector Multicast Routing Protocol • host-query—Host query • host-report—Host report • pim—Protocol Independent Multicast • trace—Multicast trace

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(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 <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 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)
fragments	<p>(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.</p>

Send comments to nexus5k-docfeedback@cisco.com

log	<p>(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information:</p> <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable
precedence <i>precedence</i>	<p>(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the <i>precedence</i> argument. The <i>precedence</i> argument can be a number or a keyword as follows:</p> <ul style="list-style-type: none"> • 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)

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

Command History

Release	Modification
5.2(1)N1(1)	Added ACL logging capability.
4.0(0)N1(1a)	This command was introduced.

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:

Send comments to nexus5k-docfeedback@cisco.com

- 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 igmp 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 igmp 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 igmp 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.

Examples

This example shows how to configure an IPv4 ACL named `acl-lab-01` with rules that deny all IGMP 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(config)# ip access-list acl-lab-01
switch(config-acl)# deny igmp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny igmp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit ip any any
```

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.

Send comments to nexus5k-docfeedback@cisco.com

deny ip (IPv4)

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

```
[sequence-number] deny ip source destination [dscp dscp | fragments | log | precedence
precedence]
```

```
no deny ip source destination [dscp dscp | fragments | log | precedence precedence]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(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 <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 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)
fragments	<p>(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.</p>

Send comments to nexus5k-docfeedback@cisco.com

log	<p>(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information:</p> <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable
precedence <i>precedence</i>	<p>(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the <i>precedence</i> argument. The <i>precedence</i> argument can be a number or a keyword as follows:</p> <ul style="list-style-type: none"> • 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)

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

Command History

Release	Modification
5.2(1)N1(1)	Added ACL logging capability.
4.0(0)N1(1a)	This command was introduced.

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:

Send comments to nexus5k-docfeedback@cisco.com

- 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 ip 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 ip 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 ip 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.

Examples

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

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# deny ip 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny ip 192.168.37.0/16 10.176.0.0/16
```

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

deny tcp (IPv4)

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

General Syntax

```
[sequence-number] deny tcp source [operator port [port] | portgroup portgroup] destination
[operator port [port] | portgroup portgroup] [dscp dscp | established | flags | fragments | log |
precedence precedence]
```

```
no deny tcp source [operator port [port] | portgroup portgroup] destination [operator port [port]
| portgroup portgroup] [dscp dscp | established | flags | fragments | log | precedence
precedence]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

<i>operator port [port]</i>	<p>(Optional) Rule that matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the <i>operator</i> and <i>port</i> arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>The <i>port</i> argument can be the name or the number of a TCP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see the “TCP Port Names” section in the “Usage Guidelines” section.</p> <p>A second <i>port</i> argument is required only when the <i>operator</i> argument is a range.</p> <p>The <i>operator</i> argument must be one of the following keywords:</p> <ul style="list-style-type: none"> • eq—Matches only if the port in the packet is equal to the <i>port</i> argument. • gt—Matches only if the port in the packet is greater than the <i>port</i> argument. • lt—Matches only if the port in the packet is less than the <i>port</i> argument. • neq—Matches only if the port in the packet is not equal to the <i>port</i> argument. • range—Requires two <i>port</i> arguments and matches only if the port in the packet is equal to or greater than the first <i>port</i> argument and equal to or less than the second <i>port</i> argument.
portgroup <i>portgroup</i>	<p>(Optional) 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 <i>portgroup</i> argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>Use the object-group ip port command to create and change IP port-group objects.</p>

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(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 <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 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)
established	<p>(Optional) 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.</p>
flags <i>flags</i>	<p>(Optional) Rule that matches only packets that have specific TCP control bit flags set. The value of the <i>flags</i> argument must be one or more of the following keywords:</p> <ul style="list-style-type: none"> • ack • fin • psh • rst • syn • urg

Send comments to nexus5k-docfeedback@cisco.com

<i>operator port [port]</i>	<p>(Optional) Rule that matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the <i>operator</i> and <i>port</i> arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>The <i>port</i> argument can be the name or the number of a TCP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see the “TCP Port Names” section in the “Usage Guidelines” section.</p> <p>A second <i>port</i> argument is required only when the <i>operator</i> argument is a range.</p> <p>The <i>operator</i> argument must be one of the following keywords:</p> <ul style="list-style-type: none"> • eq—Matches only if the port in the packet is equal to the <i>port</i> argument. • gt—Matches only if the port in the packet is greater than the <i>port</i> argument. • lt—Matches only if the port in the packet is less than the <i>port</i> argument. • neq—Matches only if the port in the packet is not equal to the <i>port</i> argument. • range—Requires two <i>port</i> arguments and matches only if the port in the packet is equal to or greater than the first <i>port</i> argument and equal to or less than the second <i>port</i> argument.
portgroup <i>portgroup</i>	<p>(Optional) 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 <i>portgroup</i> argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>Use the object-group ip port command to create and change IP port-group objects.</p>

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(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 <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 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)
established	<p>(Optional) 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.</p>
flags <i>flags</i>	<p>(Optional) Rule that matches only packets that have specific TCP control bit flags set. The value of the <i>flags</i> argument must be one or more of the following keywords:</p> <ul style="list-style-type: none"> • ack • fin • psh • rst • syn • urg

Send comments to nexus5k-docfeedback@cisco.com

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.
log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable
precedence <i>precedence</i>	(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the <i>precedence</i> argument. The <i>precedence</i> argument can be a number or a keyword as follows: <ul style="list-style-type: none"> • 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)

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

Command History

Release	Modification
5.2(1)N1(1)	Added ACL logging capability.
4.0(0)N1(1a)	This command was introduced.

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.

Send comments to nexus5k-docfeedback@cisco.com

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 tcp 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 tcp 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.

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)

Send comments to nexus5k-docfeedback@cisco.com

- **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)

Examples

This example shows how to configure an IPv4 ACL named `acl-lab-01` with rules that deny all TCP 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(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 tcp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit ip any any
```

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

deny udp (IPv4)

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

General Syntax

```
[sequence-number] deny udp source [operator port [port] | portgroup portgroup] destination
[operator port [port] | portgroup portgroup] [dscp dscp | fragments | log | precedence
precedence]
```

```
no deny udp source [operator port [port] | portgroup portgroup] destination [operator port [port]
| portgroup portgroup] [dscp dscp | fragments | log | precedence precedence]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

<i>operator port [port]</i>	<p>(Optional) Rule that matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the <i>operator</i> and <i>port</i> arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>The <i>port</i> 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.</p> <p>A second <i>port</i> argument is required only when the <i>operator</i> argument is a range.</p> <p>The <i>operator</i> argument must be one of the following keywords:</p> <ul style="list-style-type: none">• eq—Matches only if the port in the packet is equal to the <i>port</i> argument.• gt—Matches only if the port in the packet is greater than the <i>port</i> argument.• lt—Matches only if the port in the packet is less than the <i>port</i> argument.• neq—Matches only if the port in the packet is not equal to the <i>port</i> argument.• range—Requires two <i>port</i> arguments and matches only if the port in the packet is equal to or greater than the first <i>port</i> argument and equal to or less than the second <i>port</i> argument.
portgroup <i>portgroup</i>	<p>(Optional) 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 <i>portgroup</i> argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>Use the object-group ip port command to create and change IP port-group objects.</p>

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(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 <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 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)
fragments	<p>(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.</p>

Send comments to nexus5k-docfeedback@cisco.com

log	<p>(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information:</p> <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable
precedence <i>precedence</i>	<p>(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the <i>precedence</i> argument. The <i>precedence</i> argument can be a number or a keyword as follows:</p> <ul style="list-style-type: none"> • 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)

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

Command History

Release	Modification
5.2(1)N1(1)	Added ACL logging capability.
4.0(0)N1(1a)	This command was introduced.

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:

Send comments to nexus5k-docfeedback@cisco.com

- 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 udp 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 udp 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.

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)

Send comments to nexus5k-docfeedback@cisco.com

- **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)
- **xmcp**—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 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(config)# ip access-list acl-lab-01
switch(config-acl)# deny udp 10.23.0.0/16 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
```

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

deny icmp (IPv6)

To create an access control list (ACL) rule that denies ICMP IPv6 traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

```
[sequence-number] deny icmp source destination [icmp-message | dscp dscp |
flow-label flow-label-value | fragments]
```

```
no deny icmp source destination [icmp-message | dscp dscp | flow-label flow-label-value |
fragments]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.
<i>icmp-message</i>	(Optional) ICMPv6 message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed in the “ICMPv6 Message Types” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only 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)
flow-label <i>flow-label-value</i>	<p>(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the <i>flow-label-value</i> argument. The <i>flow-label-value</i> argument can be an integer from 0 to 1048575.</p>
fragments	<p>(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. 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 devices requires to evaluate those options is contained only in initial fragments.</p>

Command Default None

Send comments to nexus5k-docfeedback@cisco.com

Command Modes IPv6 ACL configuration

Command History	Release	Modification
	4.0(1a)N1(1)	This command was introduced.

Usage Guidelines A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions 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.

Source and Destination

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

- Address and variable-length subnet mask—You can use an IPv6 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:

IPv6-address/prefix-len

This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

```
switch(config-acl)# deny icmp 2001:0db8:85a3::/48 any
```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

host *IPv6-address*

This syntax is equivalent to *IPv6-address/128*.

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-acl)# deny icmp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 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.

ICMPv6 Message Types

The *icmp-message* argument can be the ICMPv6 message number, which is an integer from 0 to 255. It can also be one of the following keywords:

- beyond-scope**—Destination beyond scope
- destination-unreachable**—Destination address is unreachable
- echo-reply**—Echo reply
- echo-request**—Echo request (ping)
- header**—Parameter header problems

Send comments to nexus5k-docfeedback@cisco.com

- **hop-limit**—Hop limit exceeded in transit
- **mld-query**—Multicast Listener Discovery Query
- **mld-reduction**—Multicast Listener Discovery Reduction
- **mld-report**—Multicast Listener Discovery Report
- **nd-na**—Neighbor discovery neighbor advertisements
- **nd-ns**—Neighbor discovery neighbor solicitations
- **next-header**—Parameter next header problems
- **no-admin**—Administration prohibited destination
- **no-route**—No route to destination
- **packet-too-big**—Packet too big
- **parameter-option**—Parameter option problems
- **parameter-problem**—All parameter problems
- **port-unreachable**—Port unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—Neighbor redirect
- **renum-command**—Router renumbering command
- **renum-result**—Router renumbering result
- **renum-seq-number**—Router renumbering sequence number reset
- **router-advertisement**—Neighbor discovery router advertisements
- **router-renumbering**—All router renumbering
- **router-solicitation**—Neighbor discovery router solicitations
- **time-exceeded**—All time exceeded messages
- **unreachable**—All unreachable

Examples

This example shows how to configure an IPv6 ACL named `acl-lab13-ipv6` with rules denying all ICMP traffic from the `2001:0db8:85a3::` and `2001:0db8:69f2::` networks to the `2001:0db8:be03:2112::` network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# deny icmp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny icmp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL.
permit (IPv6)	Configures a permit rule in an IPv6 ACL.
remark	Configures a remark in an ACL.
time-range	Configures a time range.

Send comments to nexus5k-docfeedback@cisco.com

deny ipv6 (IPv6)

To create an access control list (ACL) rule that denies IPv6 traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

[sequence-number] deny ipv6 source destination [dscp dscp | fragments]

no deny ipv6 *source destination [dscp dscp | flow-label flow-label-value | fragments]*

no *sequence-number*

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only 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)
fragments	<p>(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. 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 devices requires to evaluate those options is contained only in initial fragments.</p>

Command Default None

Command Modes IPv6 ACL configuration

Send comments to nexus5k-docfeedback@cisco.com

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions 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.

Source and Destination

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

- Address and variable-length subnet mask—You can use an IPv6 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:

IPv6-address/prefix-len

This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

```
switch(config-acl)# deny ipv6 2001:0db8:85a3::/48 any
```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

host *IPv6-address*

This syntax is equivalent to *IPv6-address/128*.

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-acl)# deny ipv6 host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 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.

Examples

This example shows how to configure an IPv6 ACL named acl-lab13-ipv6 with rules denying all IPv6 traffic from the 2001:0db8:85a3:: and 2001:0db8:69f2:: networks to the 2001:0db8:be03:2112:: network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# deny ipv6 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny ipv6 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

Send comments to nexus5k-docfeedback@cisco.com

Related Commands	Command	Description
	ipv6 access-list	Configures an IPv6 ACL.
	permit (IPv6)	Configures a permit rule in an IPv6 ACL.
	remark	Configures a remark in an ACL.
	time-range	Configures a time range.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

deny sctp (IPv6)

To create an access control list (ACL) rule that denies SCTP IPv6 traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

```
[sequence-number] deny sctp source [operator port [port] | portgroup portgroup] destination
[operator port [port] | portgroup portgroup] [dscp dscp | flow-label flow-label-value |
fragments]
```

```
no deny sctp source [operator port [port] | portgroup portgroup] destination [operator port [port]
| portgroup portgroup] [dscp dscp | flow-label flow-label-value | fragments | log ]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

<i>operator port [port]</i>	<p>(Optional) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the <i>operator</i> and <i>port</i> arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>The <i>port</i> 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.</p> <p>A second <i>port</i> argument is required only when the <i>operator</i> argument is a range.</p> <p>The <i>operator</i> argument must be one of the following keywords:</p> <ul style="list-style-type: none"> • eq—Matches only if the port in the packet is equal to the <i>port</i> argument. • gt—Matches only if the port in the packet is greater than the <i>port</i> argument. • lt—Matches only if the port in the packet is less than the <i>port</i> argument. • neq—Matches only if the port in the packet is not equal to the <i>port</i> argument. • range—Requires two <i>port</i> arguments and matches only if the port in the packet is equal to or greater than the first <i>port</i> argument and equal to or less than the second <i>port</i> argument.
portgroup <i>portgroup</i>	<p>(Optional) 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 <i>portgroup</i> argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>Use the object-group ip port command to create and change IP port-group objects.</p>

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only 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)
flow-label <i>flow-label-value</i>	<p>(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the <i>flow-label-value</i> argument. The <i>flow-label-value</i> argument can be an integer from 0 to 1048575.</p>
fragments	<p>(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. 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 devices requires to evaluate those options is contained only in initial fragments.</p>

Command Default

None

Send comments to nexus5k-docfeedback@cisco.com

Command Modes IPv6 ACL configuration

Command History	Release	Modification
	4.0(1a)N1(1)	This command was introduced.

Usage Guidelines A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions 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.

Source and Destination

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

- Address and variable-length subnet mask—You can use an IPv6 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:

IPv6-address/prefix-len

This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

```
switch(config-acl)# deny sctp 2001:0db8:85a3::/48 any
```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

host *IPv6-address*

This syntax is equivalent to *IPv6-address/128*.

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-acl)# deny sctp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 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.

Examples

This example shows how to configure an IPv6 ACL named acl-lab13-ipv6 with rules denying all SCTP traffic from the 2001:0db8:85a3:: and 2001:0db8:69f2:: networks to the 2001:0db8:be03:2112:: network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# deny sctp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny sctp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

Send comments to nexus5k-docfeedback@cisco.com

Related Commands	Command	Description
	ipv6 access-list	Configures an IPv6 ACL.
	permit (IPv6)	Configures a permit rule in an IPv6 ACL.
	remark	Configures a remark in an ACL.
	time-range	Configures a time range.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

deny tcp (IPv6)

To create an access control list (ACL) rule that denies TCP IPv6 traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

General Syntax

```
[sequence-number] deny tcp source [operator port [port] | portgroup portgroup] destination
[operator port [port] | portgroup portgroup] [dscp dscp | flow-label flow-label-value |
fragments | flags | established]
```

```
no deny tcp source [operator port [port] | portgroup portgroup] destination [operator port [port]
| portgroup portgroup] [dscp dscp | flow-label flow-label-value | fragments | flags |
established]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

<i>operator port [port]</i>	<p>(Optional) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the <i>operator</i> and <i>port</i> arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>The <i>port</i> argument can be the name or the number of a TCP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see the “TCP Port Names” section in the “Usage Guidelines” section.</p> <p>A second <i>port</i> argument is required only when the <i>operator</i> argument is a range.</p> <p>The <i>operator</i> argument must be one of the following keywords:</p> <ul style="list-style-type: none"> • eq—Matches only if the port in the packet is equal to the <i>port</i> argument. • gt—Matches only if the port in the packet is greater than the <i>port</i> argument. • lt—Matches only if the port in the packet is less than the <i>port</i> argument. • neq—Matches only if the port in the packet is not equal to the <i>port</i> argument. • range—Requires two <i>port</i> arguments and matches only if the port in the packet is equal to or greater than the first <i>port</i> argument and equal to or less than the second <i>port</i> argument.
portgroup <i>portgroup</i>	<p>(Optional) 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 <i>portgroup</i> argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>Use the object-group ip port command to create and change IP port-group objects.</p>

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only 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)
flow-label <i>flow-label-value</i>	<p>(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the <i>flow-label-value</i> argument. The <i>flow-label-value</i> argument can be an integer from 0 to 1048575.</p>
fragments	<p>(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. 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 devices requires to evaluate those options is contained only in initial fragments.</p>

Send comments to nexus5k-docfeedback@cisco.com

flags (Optional) Rule 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) Specifies that the rule matches only packets that belong to an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection.

Command Default None

Command Modes IPv6 ACL configuration

Command History	Release	Modification
	4.0(1a)N1(1)	This command was introduced.

Usage Guidelines A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions 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.

Source and Destination

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

- Address and variable-length subnet mask—You can use an IPv6 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:

IPv6-address/prefix-len

This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

```
switch(config-acl)# deny tcp 2001:0db8:85a3::/48 any
```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

host *IPv6-address*

Send comments to nexus5k-docfeedback@cisco.com

This syntax is equivalent to *IPv6-address/128*.

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-acl)# deny tcp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 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.

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)
- **nnntp**—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)

Send comments to nexus5k-docfeedback@cisco.com

- **telnet**—Telnet (23)
- **time**—Time (37)
- **uucp**—Unix-to-Unix Copy Program (54)
- **whois**—WHOIS/NICNAME (43)
- **www**—World Wide Web (HTTP, 8)

Examples

This example shows how to configure an IPv6 ACL named `acl-lab13-ipv6` with rules denying all TCP traffic from the `2001:0db8:85a3::` and `2001:0db8:69f2::` networks to the `2001:0db8:be03:2112::` network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# deny tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL.
permit (IPv6)	Configures a permit rule in an IPv6 ACL.
remark	Configures a remark in an ACL.
time-range	Configures a time range.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

deny udp (IPv6)

To create an access control list (ACL) rule that denies UDP IPv6 traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command. To create an IPv6 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 udp source [operator port [port] | portgroup portgroup] destination
[operator port [port] | portgroup portgroup] [dscp dscp | flow-label flow-label-value |
fragments]
```

```
no deny udp source [operator port [port] | portgroup portgroup] destination [operator port [port]
| portgroup portgroup] [dscp dscp | flow-label flow-label-value | fragments]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

<i>operator port [port]</i>	<p>(Optional) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the <i>operator</i> and <i>port</i> arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>The <i>port</i> argument can be the name or the number of a UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see the “UDP Port Names” section in the “Usage Guidelines” section.</p> <p>A second <i>port</i> argument is required only when the <i>operator</i> argument is a range.</p> <p>The <i>operator</i> argument must be one of the following keywords:</p> <ul style="list-style-type: none"> • eq—Matches only if the port in the packet is equal to the <i>port</i> argument. • gt—Matches only if the port in the packet is greater than the <i>port</i> argument. • lt—Matches only if the port in the packet is less than the <i>port</i> argument. • neq—Matches only if the port in the packet is not equal to the <i>port</i> argument. • range—Requires two <i>port</i> arguments and matches only if the port in the packet is equal to or greater than the first <i>port</i> argument and equal to or less than the second <i>port</i> argument.
portgroup <i>portgroup</i>	<p>(Optional) 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 <i>portgroup</i> argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>Use the object-group ip port command to create and change IP port-group objects.</p>

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only 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)
flow-label <i>flow-label-value</i>	<p>(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the <i>flow-label-value</i> argument. The <i>flow-label-value</i> argument can be an integer from 0 to 1048575.</p>
fragments	<p>(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. 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 devices requires to evaluate those options is contained only in initial fragments.</p>

Command Default

None

Send comments to nexus5k-docfeedback@cisco.com

Command Modes IPv6 ACL configuration

Command History	Release	Modification
	4.0(1a)N1(1)	This command was introduced.

Usage Guidelines A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions 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.

Source and Destination

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

- Address and variable-length subnet mask—You can use an IPv6 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:

IPv6-address/prefix-len

This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

```
switch(config-acl)# deny udp 2001:0db8:85a3::/48 any
```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

host *IPv6-address*

This syntax is equivalent to *IPv6-address/128*.

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-acl)# deny udp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 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.

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)

Send comments to nexus5k-docfeedback@cisco.com

- **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)
- **xmcp**—X Display Manager Control Protocol (177)

Examples

This example shows how to configure an IPv6 ACL named `acl-lab13-ipv6` with rules denying all UDP traffic from the `2001:0db8:85a3::` and `2001:0db8:69f2::` networks to the `2001:0db8:be03:2112::` network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# deny udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL.
permit (IPv6)	Configures a permit rule in an IPv6 ACL.
remark	Configures a remark in an ACL.
time-range	Configures a time range.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

deny (MAC)

To create a Media Access Control (MAC) 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.

[sequence-number] deny source destination [protocol] [cos cos-value] [vlan vlan-id]

no deny *source destination [protocol] [cos cos-value] [vlan vlan-id]*

no *sequence-number*

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source MAC 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.
<i>destination</i>	Destination MAC 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.
<i>protocol</i>	(Optional) Protocol number that the rule matches. Valid protocol numbers are 0x0 to 0xffff. For listings of valid protocol names, see “MAC Protocols” in the “Usage Guidelines” section.
cos <i>cos-value</i>	(Optional) Specifies that the rule matches only packets whose IEEE 802.1Q header contains the class of service (CoS) value given in the <i>cos-value</i> argument. The <i>cos-value</i> argument can be an integer from 0 to 7.
vlan <i>vlan-id</i>	(Optional) Specifies that the rule matches only packets whose IEEE 802.1Q header contains the VLAN ID given. The <i>vlan-id</i> argument can be an integer from 1 to 4094.

Command Default

A newly created MAC 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

MAC ACL configuration mode

Send comments to nexus5k-docfeedback@cisco.com

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When the switch applies a MAC 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 two 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 mask—You can use a MAC address followed by a mask to specify a single address or a group of addresses. The syntax is as follows:

MAC-address MAC-mask

This example specifies the *source* argument with the MAC address 00c0.4f03.0a72:

```
switch(config-acl)# deny 00c0.4f03.0a72 0000.0000.0000 any
```

This example specifies the *destination* argument with a MAC address for all hosts with a MAC vendor code of 00603e:

```
switch(config-acl)# deny any 0060.3e00.0000 0000.0000.0000
```

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

MAC Protocols

The *protocol* argument can be the MAC protocol number or a keyword. Protocol numbers are a four-byte hexadecimal number prefixed with 0x. Valid protocol numbers are from 0x0 to 0xffff. Valid keywords are the following:

- aarp**—Appletalk ARP (0x80f3)
- appletalk**—Appletalk (0x809b)
- decnet-iv**—DECnet Phase IV (0x6003)
- diagnostic**—DEC Diagnostic Protocol (0x6005)
- etype-6000**—EtherType 0x6000 (0x6000)
- etype-8042**—EtherType 0x8042 (0x8042)
- ip**—Internet Protocol v4 (0x0800)
- lat**—DEC LAT (0x6004)
- larc-sca**—DEC LARC, SCA (0x6007)
- mop-console**—DEC MOP Remote console (0x6002)
- mop-dump**—DEC MOP dump (0x6001)
- vines-echo**—VINES Echo (0x0baf)

Send comments to nexus5k-docfeedback@cisco.com

Examples

This example shows how to configure a MAC ACL named mac-ip-filter with rules that permit any non-IPv4 traffic between two groups of MAC addresses:

```
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# deny 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
switch(config-mac-acl)# permit any any
```

Related Commands

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

Send comments to nexus5k-docfeedback@cisco.com

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	<i>text</i>	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
	4.0(0)N1(1a)	This command was introduced.

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

Examples	<p>This example shows how to configure the description for a user role:</p> <pre>switch(config)# role name MyRole switch(config-role)# description User role for my user account.</pre> <p>This example shows how to remove the description from a user role:</p> <pre>switch(config)# role name MyRole switch(config-role)# no description</pre>
----------	---

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

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com



E Commands

This chapter describes the Cisco NX-OS security commands that begin with E.

Send comments to nexus5k-docfeedback@cisco.com

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	<i>level</i>	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(2)N1(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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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-lvl*]

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

Syntax Description	0	(Optional) Specifies that the password is in clear text.
	5	(Optional) Specifies that the password is in encrypted format.
	<i>password</i>	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 <i>priv-lvl</i>	(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(2)N1(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.

Send comments to nexus5k-docfeedback@cisco.com

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.

Send comments to nexus5k-docfeedback@cisco.com



F Commands

This chapter describes the Cisco NX-OS security commands that begin with F.

Send comments to nexus5k-docfeedback@cisco.com

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	<i>feature-name</i> 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
	4.0(0)N1(1a)	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:	
	<pre>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</pre>	
Related Commands	This example shows how to remove a feature from a user role feature group:	
	<pre>switch(config)# role feature-group name MyGroup switch(config-role-featuregrp)# no feature callhome</pre>	
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.

Send comments to nexus5k-docfeedback@cisco.com

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(2)N2(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 DHCP snooping are unavailable.

Dynamic ARP inspection and IP Source Guard depend 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)
- IP Source Guard

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

This example shows how to disable DHCP snooping:

Send comments to nexus5k-docfeedback@cisco.com

```
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, including IP Source Guard configuration.

Send comments to nexus5k-docfeedback@cisco.com

feature http-server

To enable HTTP or Hypertext Transfer Protocol Secure (HTTPS) on the switch, use the **feature http-server** command. To disable the HTTP or HTTPS server, use the **no** form of this command.

feature http-server

no feature http-server

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration mode

Command History	Release	Modification
	5.0(2)N1(1)	This command was introduced.

Usage Guidelines In releases earlier than Cisco NX-OS Release 5.0(2)N1(1), HTTP and HTTPS are enabled on the switch by default.

Examples This example shows how to enable the HTTP server on the switch and verify the status of the HTTP server:

```
switch(config)# feature http-server
switch(config)# exit
switch# show feature
Feature Name      Instance  State
-----
assoc_mgr         1         enabled
cimserver         1         disabled
dhcp-snooping    1         disabled
fabric-binding    1         disabled
fc-port-security  1         disabled
fcoe              1         enabled
fcsp              1         disabled
fex               1         enabled
fport-channel-trunk 1         disabled
http-server       1         enabled
interface-vlan    1         enabled
lACP              1         enabled
ldap              1         disabled
lldp              1         enabled
niv               1         disabled
npiv              1         disabled
npv               1         disabled
otv               1         disabled
port_track       1         disabled
```

Send comments to nexus5k-docfeedback@cisco.com

```
private-vlan      1      enabled
privilege         1      enabled
sshServer         1      enabled
tacacs            1      enabled
telnetServer      1      enabled
udld              1      enabled
vpc               1      enabled
vtp               1      enabled
switch# show http-server
http-server enabled
switch#
```

Related Commands	Command	Description
	copy running-config startup-config	Copies the running configuration to the startup configuration.
	show feature	Displays the features enabled or disabled on the switch.
	show http-server	Displays the HTTP or HTTPS server configuration.

Send comments to nexus5k-docfeedback@cisco.com

feature port-security

To enable port security on Layer 2 interfaces, use the **feature port-security** command. To disable port security, use the **no** form of this command.

feature port-security

no feature port-security

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	Disabled
------------------------	----------

Command Modes	Global configuration mode
----------------------	---------------------------

Command History	Release	Modification
	5.1(3)N1(1)	This command was introduced.

Usage Guidelines	Use the port security feature to secure a port by limiting and identifying the MAC addresses of the switches that are allowed to access the port.
-------------------------	---

You can enable port security on a virtual port channel (vPC) port only if the following occurs:

- Port security is enabled on both the vPC peers
- Port security is enabled on the vPC port on both the vPC peers.

This command does not require a license.

Examples	This example shows how to enable port security on the switch:
-----------------	---

```
switch# configure terminal
switch(config)# feature port-security
switch(config)#
```

This example shows how to disable port security on the switch:

```
switch# configure terminal
switch(config)# no feature port-security
switch(config)#
```

Related Commands	Command	Description
	show feature	Displays the features that are enabled or disabled on the switch.

Send comments to nexus5k-docfeedback@cisco.com

Command	Description
show port-security	Displays the port security configuration information.
switchport port-security	Configures the switchport parameters to establish port security.

Send comments to nexus5k-docfeedback@cisco.com

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(2)N1(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(config)# feature privilege  
switch(config)#
```

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

```
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.

Send comments to nexus5k-docfeedback@cisco.com

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
4.0(0)N1(1a)	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(config)# feature tacacs+
```

This example shows how to disable TACACS+:

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

Related Commands

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

Send comments to nexus5k-docfeedback@cisco.com



I Commands

This chapter describes the Cisco NX-OS security commands that begin with I.

Send comments to nexus5k-docfeedback@cisco.com

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
4.0(0)N1(1a)	This command was introduced.

Examples

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

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

Related Commands

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

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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

<i>access-list-name</i>	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 5000 Series switch and the addresses in the access list.
out	Specifies that outgoing connections be restricted between a particular Cisco Nexus 5000 Series switch and the addresses in the access list.

Command Default

None

Command Modes

Line configuration mode

Command History

Release	Modification
5.0(2)N1(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.

Send comments to nexus5k-docfeedback@cisco.com

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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**

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

Syntax Description	<i>access-list-name</i>	Name of the IPv4 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
	in	Specifies that the ACL applies to inbound traffic.

Command Default	None
-----------------	------

Command Modes	Interface configuration mode Subinterface configuration mode
---------------	---

Command History	Release	Modification
	5.0(3)N1(1)	This command was introduced.

Usage Guidelines	By default, no IPv4 ACLs are applied to a Layer 3 routed interface.
	<p>You can use the ip access-group command to apply an IPv4 ACL as a router ACL to the following interface types:</p> <ul style="list-style-type: none">• VLAN interfaces• Layer 3 Ethernet interfaces• Layer 3 Ethernet subinterfaces• Layer 3 Ethernet port-channel interfaces and subinterfaces• Loopback interfaces• Management interfaces <p>You can also use the ip access-group command to apply an IPv4 ACL as a router ACL to the following interface types:</p> <ul style="list-style-type: none">• Layer 2 Ethernet interfaces• Layer 2 Ethernet port-channel interfaces <p>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.</p> <p>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.</p> <p>A router ACL can be applied only to ingress traffic.</p>

Send comments to nexus5k-docfeedback@cisco.com

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
```

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
```

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.

Send comments to nexus5k-docfeedback@cisco.com

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

<i>access-list-name</i>	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

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

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.

Examples

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

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

Send comments to nexus5k-docfeedback@cisco.com

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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(2)N1(1)	This command was introduced.

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

```
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(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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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 <i>number</i> 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)N1(1)	This command was introduced.
Usage Guidelines	<p>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.</p> <p>By default, the DAI logging buffer size is 32 messages.</p>	
Examples	<p>This example shows how to configure the DAI logging buffer size:</p> <pre>switch# configure terminal switch(config)# ip arp inspection log-buffer entries 64 switch(config)#</pre>	
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.

Send comments to nexus5k-docfeedback@cisco.com

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)N1(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.

Send comments to nexus5k-docfeedback@cisco.com

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(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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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		
<i>vlan-list</i>		VLANs on which DAI is active. The <i>vlan-list</i> 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. <ul style="list-style-type: none"> 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)N1(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)#
```

Send comments to nexus5k-docfeedback@cisco.com

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.

Send comments to nexus5k-docfeedback@cisco.com

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)N1(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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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(2)N2(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 DHCP 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.

Send comments to nexus5k-docfeedback@cisco.com

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(2)N2(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, including IP Source Guard configuration.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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(2)N2(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, including IP Source Guard configuration.

Send comments to nexus5k-docfeedback@cisco.com

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(2)N2(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, including IP Source Guard configuration.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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(2)N2(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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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

<i>vlan-list</i>	Range of VLANs on which to enable DHCP snooping. The <i>vlan-list</i> 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(2)N2(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, including IP Source Guard configuration.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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

<i>access-list-name</i>	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
Virtual Ethernet interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
5.1(3)N1(1)	Support for this command was introduced for virtual Ethernet interfaces.

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
- Virtual Ethernet interface

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

Send comments to nexus5k-docfeedback@cisco.com

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

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

This example shows how to apply an IPv4 ACL named ip-acl-03 to the virtual Ethernet interface 1 as a port ACL:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# ip port access-group ip-acl-03 in
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	<i>IP-address</i>	IPv4 address to be used on the specified interface. Valid entries are in dotted-decimal format.
	<i>MAC-address</i>	MAC address to be used on the specified interface. Valid entries are in dotted-hexadecimal format.
	vlan <i>vlan-id</i>	Specifies the VLAN associated with the IP source entry.
	interface ethernet <i>slot/port</i>	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 <i>channel-no</i>	Specifies the EtherChannel interface. The number can be from 1 to 4096.

Command Default None

Command Modes Global configuration mode

Command History	Release	Modification
	5.0(2)N2(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)#
```

Send comments to nexus5k-docfeedback@cisco.com

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

ip verify source dhcp-snooping-vlan

To enable IP Source Guard on a Layer 2 Ethernet interface, use the **ip verify source dhcp-snooping-vlan** command. To disable IP Source Guard on a Layer 2 Ethernet interface, use the **no** form of this command.

ip verify source dhcp-snooping-vlan

no ip verify source dhcp-snooping-vlan

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Interface configuration mode

Release	Modification
5.0(3)N1(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.

IP Source Guard limits IP traffic on an interface to only those sources that have an IP-MAC address binding table entry or static IP source entry.

IP Source Guard is dependent upon DHCP snooping to build and maintain the IP-MAC address binding table or upon manual maintenance of static IP source entries.

This command does not require a license.

Examples This example shows how to enable IP Source Guard on a Layer 2 interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# ip verify source dhcp-snooping-vlan
switch(config-if)#
```

This example shows how to disable IP Source Guard on a Layer 2 interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no ip verify source dhcp-snooping-vlan
switch(config-if)#
```

Send comments to nexus5k-docfeedback@cisco.com

Related Commands	Command	Description
	feature dhcp	Enables DHCP snooping on the switch.
	ip source binding	Creates a static IP source entry for a Layer 2 Ethernet interface.
	show ip verify source	Displays the IP-to-MAC address bindings for an interface.
	show running-config dhcp	Displays the IP configuration in the running configuration.
	show running-config interface ethernet	Displays the interface configuration in the running configuration.

Send comments to nexus5k-docfeedback@cisco.com

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)N1(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)# ip verify unicast source reachable-via any
```

Send comments to nexus5k-docfeedback@cisco.com

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
```

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.

Send comments to nexus5k-docfeedback@cisco.com

ipv6 access-class

To create or configure an IPv6 access class to restrict incoming or outgoing traffic on a virtual terminal line (VTY), use the **ipv6 access-class** command. To remove the access class, use the **no** form of this command.

ipv6 access-class *access-list-name* {**in** | **out**}

no ipv6 access-class *access-list-name* {**in** | **out**}

Syntax Description

<i>access-list-name</i>	Name of the IPv6 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 5000 Series switch and the addresses in the access list.
out	Specifies that outgoing connections be restricted between a particular Cisco Nexus 5000 Series switch and the addresses in the access list.

Command Default

None

Command Modes

Line configuration mode

Command History

Release	Modification
5.0(2)N1(1)	This command was introduced.

Examples

This example shows how to configure an IPv6 access class on a VTY line to restrict inbound packets:

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# ipv6 access-class VTY_I6ACCESS in
switch(config-line)#
```

This example shows how to remove an IPv6 access class that restricts inbound packets:

```
switch(config)# line vty
switch(config-line)# no ipv6 access-class VTY_I6ACCESS 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 ipv6 access-class	Displays IPv6 access classes.

Send comments to nexus5k-docfeedback@cisco.com

Command	Description
show line	Displays the access lists for a particular terminal line.
show running-config aclmgr	Displays the running configuration of ACLs.
show startup-config aclmgr	Displays the startup configuration for ACLs.
ssh6	Starts an SSH session using IPv6.
telnet6	Starts a Telnet session using IPv6.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

ipv6 access-list

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

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

Syntax Description	<i>access-list-name</i>	Name of the IPv6 ACL, which can be up to 64 alphanumeric characters long. The name cannot contain a space or quotation mark.
--------------------	-------------------------	--

Command Default	No IPv6 ACLs are defined by default.
-----------------	--------------------------------------

Command Modes	Global configuration mode
---------------	---------------------------

Command History	Release	Modification
	4.0(1a)N1(1)	This command was introduced.

Usage Guidelines	Use IPv6 ACLs to filter IPv6 traffic.
	When you use the ipv6 access-list command, the switch enters IP access list configuration mode, where you can use the IPv6 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.

Every IPv6 ACL has the following implicit rule as its last rule:

deny ipv6 any any

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

Examples	This example shows how to enter IP access list configuration mode for an IPv6 ACL named ipv6-acl-01:
	switch(config)# ipv6 access-list ipv6-acl-01
	switch(config-ipv6-acl)#

Related Commands	Command	Description
	deny (IPv6)	Configures a deny rule in an IPv6 ACL.
	permit (IPv6)	Configures a permit rule in an IPv6 ACL.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

ipv6 port traffic-filter

To apply an IPv6 access control list (ACL) to an interface as a port ACL, use the **ipv6 port traffic-filter** command. To remove an IPv6 ACL from an interface, use the **no** form of this command.

ipv6 port traffic-filter *access-list-name* **in**

no ipv6 port traffic-filter *access-list-name* **in**

Syntax Description	<i>access-list-name</i>	Name of the IPv6 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
	in	Specifies that the device applies the ACL to inbound traffic.

Command Default	None
-----------------	------

Command Modes	Interface configuration mode Virtual Ethernet interface configuration mode
---------------	---

Command History	Release	Modification
	4.0(1a)N1(1)	This command was introduced.
	5.1(3)N1(1)	Support for this command was introduced for virtual Ethernet interfaces.

Usage Guidelines	By default, no IPv6 ACLs are applied to an interface.
	You can use the ipv6 port traffic-filter command to apply an IPv6 ACL as a port ACL to the following interface types:

- Ethernet interfaces
- EtherChannel interfaces
- Virtual Ethernet interface

You can also use the **ipv6 port traffic-filter** command to apply an IPv6 ACL as a port ACL to the following interface types:

- VLAN interfaces



Note

You must enable VLAN interfaces globally before you can configure a VLAN interface. For more information, see the **feature interface-vlan** 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.

Send comments to nexus5k-docfeedback@cisco.com

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.

Examples

This example shows how to apply an IPv6 ACL named ipv6-acl to Ethernet interface 1/3:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# ipv6 port traffic-filter ipv6-acl in
switch(config-if)#
```

This example shows how to remove an IPv6 ACL named ipv6-acl from Ethernet interface 1/3:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# no ipv6 port traffic-filter ipv6-acl in
switch(config-if)#
```

This example shows how to apply an IPv6 ACL named ipv6-acl-03 to a specific virtual Ethernet interface:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# ipv6 port traffic-filter ipv6-acl-03 in
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
ipv6 access-list	Configures an IPv6 ACL.
show access-lists	Displays all ACLs.
show ipv6 access-lists	Shows either a specific IPv6 ACL or all IPv6 ACLs.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

ipv6 traffic-filter

To apply an IPv6 access control list (ACL) to an interface, use the **ipv6 traffic-filter** command. To remove an IPv6 ACL from an interface, use the **no** form of this command.

ipv6 traffic-filter *access-list-name* **in**

no ipv6 traffic-filter *access-list-name* **in**

Syntax Description	<i>access-list-name</i>	Name of the IPv6 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
	in	Specifies that the device applies the ACL to inbound traffic.

Command Default	None
-----------------	------

Command Modes	Interface configuration mode Virtual Ethernet interface configuration mode
---------------	---

Command History	Release	Modification
	4.0(1a)N1(1)	This command was introduced.
	5.1(3)N1(1)	Support for this command was introduced for virtual Ethernet interfaces.

Usage Guidelines	By default, no IPv6 ACLs are applied to an interface.
	You can use the ipv6 traffic-filter command to apply an IPv6 ACL to the following interface types: <ul style="list-style-type: none">• Ethernet interfaces• EtherChannel interfaces• Virtual Ethernet interface• VLAN interfaces



Note

You must enable VLAN interfaces globally before you can configure a VLAN interface. For more information, see the **feature interface-vlan** command.

The switch applies 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 device without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

Send comments to nexus5k-docfeedback@cisco.com

Examples

This example shows how to apply an IPv6 ACL named ipv6-acl to Ethernet interface 1/3:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# ipv6 traffic-filter ipv6-acl in
switch(config-if)#
```

This example shows how to remove an IPv6 ACL named ipv6-acl from Ethernet interface 1/3:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# no ipv6 traffic-filter ipv6-acl in
switch(config-if)#
```

This example shows how to apply an IPv6 ACL named ipv6-acl-03 to a specific virtual Ethernet interface:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# ipv6 traffic-filter ipv6-acl-03 in
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
ipv6 access-list	Configures an IPv6 ACL.
show access-lists	Displays all ACLs.
show ipv6 access-lists	Shows either a specific IPv6 ACL or all IPv6 ACLs.

Send comments to nexus5k-docfeedback@cisco.com



M Commands

This chapter describes the Cisco NX-OS security commands that begin with M.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

mac access-list

To create a Media Access Control (MAC) access control list (ACL) or to enter MAC access list configuration mode for a specific ACL, use the **mac access-list** command. To remove a MAC ACL, use the **no** form of this command.

mac access-list *access-list-name*

no mac access-list *access-list-name*

Syntax Description

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

Command Default

No MAC ACLs are defined by default.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Use MAC ACLs to filter non-IP traffic.

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

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

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

deny any any protocol

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

Examples

This example shows how to enter MAC access list configuration mode for a MAC ACL named mac-acl-01:

```
switch(config)# mac access-list mac-acl-01
switch(config-acl)#
```

Related Commands

Command	Description
deny (MAC)	Configures a deny rule in a MAC ACL.
mac access-group	Applies a MAC ACL to an interface.

Send comments to nexus5k-docfeedback@cisco.com

Command	Description
permit (MAC)	Configures a permit rule in a MAC ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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

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

Command Default

None

Command Modes

Interface configuration mode
Virtual Ethernet interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
5.1(3)N1(1)	Support for this command was added for virtual Ethernet interfaces.

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

Send comments to nexus5k-docfeedback@cisco.com

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

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

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

This example shows how to apply a MAC ACL named mac-acl-03 to a specific virtual Ethernet interface:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# mac port access-group mac-acl-03
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs.
show mac access-lists	Shows either a specific MAC ACL or all MAC ACLs.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.

Send comments to nexus5k-docfeedback@cisco.com

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** | **ipv6** | **mac**} **address** *access-list-name*

no match {**ip** | **ipv6** | **mac**} **address** *access-list-name*

Syntax Description

ip	Specifies an IPv4 ACL.
ipv6	Specifies an IPv6 ACL.
mac	Specifies a MAC ACL.
address <i>access-list-name</i>	Specifies the IPv4, IPv6, or MAC address and the access list name. The name can be up to 64 alphanumeric, case-sensitive characters long.

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

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

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

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(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
```

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.

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com



P Commands

This chapter describes the Cisco NX-OS security commands that begin with P.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

permit icmp (IPv4)

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

Need to test this: *sequence-number* **permit icmp** *source destination [icmp-message]*

[sequence-number] **permit icmp** *source destination [icmp-message | dscp dscp | fragments | log | precedence precedence]*

no permit icmp *source destination [icmp-message | dscp dscp | fragments | log | precedence precedence]*

no *sequence-number*



Note

You can also specify the **icmp** keyword by its protocol number. Valid numbers are from 0 to 255.

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ iSource and Destination ” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ iSource and Destination ” section in the “Usage Guidelines” section.
<i>icmp-message</i>	ICMP message number, which is an integer from 0 to 255, or a keyword. For a list of keywords, see the “ ICMP Message Types ” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(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 <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 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)
fragments	<p>(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.</p>

Send comments to nexus5k-docfeedback@cisco.com

log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable
precedence <i>precedence</i>	(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the <i>precedence</i> argument. The <i>precedence</i> argument can be a number or a keyword as follows: <ul style="list-style-type: none"> • 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)

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

Command History

Release	Modification
5.2(1)N1(1)	Added ACL logging capability.
4.0(0)N1(1a)	This command was introduced.

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.

iSource 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:

Send comments to nexus5k-docfeedback@cisco.com

- **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 icmp 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 icmp 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)# permit 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:

- **administrativelyprohibited**—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

Send comments to nexus5k-docfeedback@cisco.com

- **host-unknown**—Host unknown
- **host-unreachable**—Host unreachable
- **information-reply**—Information replies
- **information-request**—Information requests
- **log**—Log matches against this entry
- **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

Examples

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

```
switch(config)# ip access-list acl-lab-01
switch(config)# permit icmp 10.23.0.0/16 10.176.0.0/16
switch(config)# permit icmp 192.168.37.0/16 10.176.0.0/16
```

Send comments to nexus5k-docfeedback@cisco.com

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

permit igmp (IPv4)

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

[sequence-number] permit igmp source destination [igmp-message | dscp dscp | fragments | log | precedence precedence]

no permit igmp *source destination [igmp-message | dscp dscp | fragments | log | precedence precedence]*

no *sequence-number*



Note

You can also specify the **igmp** keyword by its protocol number. Valid numbers are from 0 to 255.

Syntax Description

<i>sequence-number</i>	(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.
igmp	Specifies that the rule applies to IGMP traffic only. When you use this keyword, the <i>igmp-message</i> argument is available.
<i>source</i>	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” in the “Usage Guidelines” section.
<i>igmp-message</i>	(Optional) Rule that matches only packets of the specified IGMP message type. The <i>igmp-message</i> argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords: <ul style="list-style-type: none"> • dvmrp—Distance Vector Multicast Routing Protocol • host-query—Host query • host-report—Host report • log—Log matches against this entry • pim—Protocol Independent Multicast • trace—Multicast trace

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(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 <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 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)
fragments	<p>(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.</p>

Send comments to nexus5k-docfeedback@cisco.com

log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable
precedence <i>precedence</i>	(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the <i>precedence</i> argument. The <i>precedence</i> argument can be a number or a keyword as follows: <ul style="list-style-type: none"> • 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)

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

Command History

Release	Modification
5.2(1)N1(1)	Added ACL logging capability.
4.0(0)N1(1a)	This command was introduced.

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:

Send comments to nexus5k-docfeedback@cisco.com

- 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 igmp 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 igmp 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)# permit igmp 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.

Examples

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

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# permit igmp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit igmp 192.168.37.0/16 10.176.0.0/16
```

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.

Send comments to nexus5k-docfeedback@cisco.com

permit ip (IPv4)

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

[sequence-number] **permit ip** *source destination* [**dscp** *dscp* | **fragments** | **log** | **precedence** *precedence*]

no permit ip *source destination* [**dscp** *dscp* | **fragments** | **log** | **precedence** *precedence*]

no *sequence-number*

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.
<i>destination</i>	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.

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(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 <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 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)
fragments	<p>(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.</p>

Send comments to nexus5k-docfeedback@cisco.com

log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable
precedence <i>precedence</i>	(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the <i>precedence</i> argument. The <i>precedence</i> argument can be a number or a keyword as follows: <ul style="list-style-type: none"> • 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)

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

Command History

Release	Modification
5.2(1)N1(1)	Added ACL logging capability.
4.0(0)N1(1a)	This command was introduced.

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:

Send comments to nexus5k-docfeedback@cisco.com

- 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 ip 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 ip 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)# permit ip 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.

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(config)# ip access-list acl-lab-01
switch(config-acl)# permit ip 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit ip 192.168.37.0/16 10.176.0.0/16
```

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

permit tcp (IPv4)

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

```
[sequence-number] permit tcp source [operator port [port] | portgroup portgroup] destination
[operator port [port] | portgroup portgroup] [dscp dscp | fragments | log | precedence
precedence | flags | established]
```

```
no permit tcp source [operator port [port] | portgroup portgroup] destination [operator port [port]
| portgroup portgroup] [dscp dscp | fragments | log | precedence precedence | flags |
established]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

<i>operator port [port]</i>	<p>(Optional) Rule that matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the <i>operator</i> and <i>port</i> arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>The <i>port</i> argument can be the name or the number of a TCP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see the “TCP Port Names” section in the “Usage Guidelines” section.</p> <p>A second <i>port</i> argument is required only when the <i>operator</i> argument is a range.</p> <p>The <i>operator</i> argument must be one of the following keywords:</p> <ul style="list-style-type: none">• eq—Matches only if the port in the packet is equal to the <i>port</i> argument.• gt—Matches only if the port in the packet is greater than the <i>port</i> argument.• lt—Matches only if the port in the packet is less than the <i>port</i> argument.• neq—Matches only if the port in the packet is not equal to the <i>port</i> argument.• range—Requires two <i>port</i> arguments and matches only if the port in the packet is equal to or greater than the first <i>port</i> argument and equal to or less than the second <i>port</i> argument.
portgroup <i>portgroup</i>	<p>(Optional) 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 <i>portgroup</i> argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>Use the object-group ip port command to create and change IP port-group objects.</p>

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(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 <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 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)
fragments	<p>(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.</p>
log	<p>(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information:</p> <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable

Send comments to nexus5k-docfeedback@cisco.com

<i>operator port [port]</i>	<p>(Optional) Rule that matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the <i>operator</i> and <i>port</i> arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>The <i>port</i> argument can be the name or the number of a TCP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see the “TCP Port Names” section in the “Usage Guidelines” section.</p> <p>A second <i>port</i> argument is required only when the <i>operator</i> argument is a range.</p> <p>The <i>operator</i> argument must be one of the following keywords:</p> <ul style="list-style-type: none">• eq—Matches only if the port in the packet is equal to the <i>port</i> argument.• gt—Matches only if the port in the packet is greater than the <i>port</i> argument.• lt—Matches only if the port in the packet is less than the <i>port</i> argument.• neq—Matches only if the port in the packet is not equal to the <i>port</i> argument.• range—Requires two <i>port</i> arguments and matches only if the port in the packet is equal to or greater than the first <i>port</i> argument and equal to or less than the second <i>port</i> argument.
portgroup <i>portgroup</i>	<p>(Optional) 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 <i>portgroup</i> argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>Use the object-group ip port command to create and change IP port-group objects.</p>

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(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 <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 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)
fragments	<p>(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.</p>
log	<p>(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information:</p> <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable

Send comments to nexus5k-docfeedback@cisco.com

precedence <i>precedence</i>	<p>(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the <i>precedence</i> argument. The <i>precedence</i> argument can be a number or a keyword as follows:</p> <ul style="list-style-type: none"> 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)
<i>flags</i>	<p>(Optional) Rule that matches only packets that have specific TCP control bit flags set. The value of the <i>flags</i> argument must be one or more of the following keywords:</p> <ul style="list-style-type: none"> ack fin psh rst syn urg
established	<p>(Optional) 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.</p>

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

Command History

Release	Modification
5.2(1)N1(1)	Added ACL logging capability.
4.0(0)N1(1a)	This command was introduced.

Send comments to nexus5k-docfeedback@cisco.com

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 tcp 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)# permit tcp 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.

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)

Send comments to nexus5k-docfeedback@cisco.com

- **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)

Examples

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

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# permit tcp 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
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
ip access-list	Configures an IPv4 ACL.

Send comments to nexus5k-docfeedback@cisco.com

Command	Description
remark	Configures a remark in an ACL.
show ip access-lists	Displays all IPv4 ACLs or one IPv4 ACL.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

permit udp (IPv4)

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

General Syntax

```
[sequence-number] permit udp source [operator port [port] | portgroup portgroup] destination
[operator port [port] | portgroup portgroup] [dscp dscp | fragments | log | precedence
precedence]
```

```
no permit udp source [operator port [port] | portgroup portgroup] destination [operator port
[port] | portgroup portgroup] [dscp dscp | fragments | log | precedence precedence]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

<i>operator port [port]</i>	<p>(Optional) Rule that matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the <i>operator</i> and <i>port</i> arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>The <i>port</i> argument can be the name or the number of a UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see the “UDP Port Names” section in the “Usage Guidelines” section.</p> <p>A second <i>port</i> argument is required only when the <i>operator</i> argument is a range.</p> <p>The <i>operator</i> argument must be one of the following keywords:</p> <ul style="list-style-type: none"> • eq—Matches only if the port in the packet is equal to the <i>port</i> argument. • gt—Matches only if the port in the packet is greater than the <i>port</i> argument. • lt—Matches only if the port in the packet is less than the <i>port</i> argument. • neq—Matches only if the port in the packet is not equal to the <i>port</i> argument. • range—Requires two <i>port</i> arguments and matches only if the port in the packet is equal to or greater than the first <i>port</i> argument and equal to or less than the second <i>port</i> argument.
portgroup <i>portgroup</i>	<p>(Optional) 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 <i>portgroup</i> argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>Use the object-group ip port command to create and change IP port-group objects.</p>

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(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 <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 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)
fragments	<p>(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.</p>

Send comments to nexus5k-docfeedback@cisco.com

log	<p>(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information:</p> <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable
precedence <i>precedence</i>	<p>(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the <i>precedence</i> argument. The <i>precedence</i> argument can be a number or a keyword as follows:</p> <ul style="list-style-type: none"> • 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)

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

Command History

Release	Modification
5.2(1)N1(1)	Added ACL logging capability.
4.0(0)N1(1a)	This command was introduced.

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:

Send comments to nexus5k-docfeedback@cisco.com

- 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 udp 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 192.168.67.132 IPv4 address:

```
switch(config-acl)# permit udp 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.

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)

Send comments to nexus5k-docfeedback@cisco.com

- **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 UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network:

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

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.

Send comments to nexus5k-docfeedback@cisco.com

permit icmp (IPv6)

To create an access control list (ACL) rule that permits IPv6 ICMP traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

General Syntax

```
[sequence-number] permit icmp source destination [icmp-message | dscp dscp |  
flow-label flow-label-value | fragments | log]
```

```
no permit permit icmp source destination [icmp-message | dscp dscp | flow-label flow-label-value  
| fragments | log]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only 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)
flow-label <i>flow-label-value</i>	<p>(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the <i>flow-label-value</i> argument. The <i>flow-label-value</i> argument can be an integer from 0 to 1048575.</p>
fragments	<p>(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. 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 devices requires to evaluate those options is contained only in initial fragments.</p>

Send comments to nexus5k-docfeedback@cisco.com

<i>icmp-message</i>	(Optional) ICMPv6 message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed under the “ ICMPv6 Message Types ” section in the “Usage Guidelines” section.
log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable

Command Default None

Command Modes IPv6 ACL configuration mode

Command History	Release	Modification
	5.2(1)N1(1)	Added ACL logging capability.
	4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions 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.

Source and Destination

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

- Address and variable-length subnet mask—You can use an IPv6 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:

IPv6-address/prefix-len

This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

```
switch(config-ipv6-acl)# permit icmp 2001:0db8:85a3::/48 any
```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

host *IPv6-address*

This syntax is equivalent to *IPv6-address/128*.

Send comments to nexus5k-docfeedback@cisco.com

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-ipv6-acl)# permit icmp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 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.

ICMPv6 Message Types

The *icmp-message* argument can be the ICMPv6 message number, which is an integer from 0 to 255. It can also be one of the following keywords:

- **beyond-scope**—Destination beyond scope
- **destination-unreachable**—Destination address is unreachable
- **echo-reply**—Echo reply
- **echo-request**—Echo request (ping)
- **header**—Parameter header problems
- **hop-limit**—Hop limit exceeded in transit
- **mld-query**—Multicast Listener Discovery Query
- **mld-reduction**—Multicast Listener Discovery Reduction
- **mld-report**—Multicast Listener Discovery Report
- **nd-na**—Neighbor discovery neighbor advertisements
- **nd-ns**—Neighbor discovery neighbor solicitations
- **next-header**—Parameter next header problems
- **no-admin**—Administration prohibited destination
- **no-route**—No route to destination
- **packet-too-big**—Packet too big
- **parameter-option**—Parameter option problems
- **parameter-problem**—All parameter problems
- **port-unreachable**—Port unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—Neighbor redirect
- **renum-command**—Router renumbering command
- **renum-result**—Router renumbering result
- **renum-seq-number**—Router renumbering sequence number reset
- **router-advertisement**—Neighbor discovery router advertisements
- **router-renumbering**—All router renumbering
- **router-solicitation**—Neighbor discovery router solicitations
- **time-exceeded**—All time exceeded messages
- **unreachable**—All unreachable

Send comments to nexus5k-docfeedback@cisco.com

Examples

This example shows how to configure an IPv6 ACL named `acl-lab13-ipv6` with rules permitting all ICMP traffic from the `2001:0db8:85a3::` and `2001:0db8:69f2::` networks to the `2001:0db8:be03:2112::` network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# permit icmp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit icmp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

Related Commands

Command	Description
deny (IPv6)	Configures a deny rule in an IPv6 ACL.
ipv6 access-list	Configures an IPv6 ACL.
remark	Configures a remark in an ACL.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

permit ipv6 (IPv6)

To create an access control list (ACL) rule that permits IPv6 traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

General Syntax

[sequence-number] **permit ipv6** *source destination* [**dscp** *dscp* | **flow-label** *flow-label-value* | **fragments** | **log**]

no permit ipv6 *source destination* [**dscp** *dscp* | **flow-label** *flow-label-value* | **fragments** | **log**]

no *sequence-number*

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only 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)
flow-label <i>flow-label-value</i>	<p>(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the <i>flow-label-value</i> argument. The <i>flow-label-value</i> argument can be an integer from 0 to 1048575.</p>

Send comments to nexus5k-docfeedback@cisco.com

fragments	(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. 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 devices requires to evaluate those options is contained only in initial fragments.
log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable

Command Default	None
------------------------	------

Command Modes	IPv6 ACL configuration mode
----------------------	-----------------------------

Command History	Release	Modification
	5.2(1)N1(1)	Added ACL logging capability.
	4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions 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.

Source and Destination

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

- Address and variable-length subnet mask—You can use an IPv6 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:

IPv6-address/prefix-len

This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

```
switch(config-acl)# permit ipv6 2001:0db8:85a3::/48 any
```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

host *IPv6-address*

Send comments to nexus5k-docfeedback@cisco.com

This syntax is equivalent to *IPv6-address/128*.

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-acl)# permit ipv6 host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 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.

Examples

This example shows how to configure an IPv6 ACL named `acl-lab13-ipv6` with rules permitting all IPv6 traffic from the 2001:0db8:85a3:: and 2001:0db8:69f2:: networks to the 2001:0db8:be03:2112:: network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# permit ipv6 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit ipv6 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

This example shows how to configure an IPv6 ACL named `ipv6-eng-to-marketing` with a rule that permits all IPv6 traffic from an IPv6-address object group named `eng_ipv6` to an IPv6-address object group named `marketing_group`:

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# permit ipv6 addrgroup eng_ipv6 addrgroup marketing_group
```

Related Commands

Command	Description
deny (IPv6)	Configures a deny rule in an IPv6 ACL.
ipv6 access-list	Configures an IPv6 ACL.
remark	Configures a remark in an ACL.

Send comments to nexus5k-docfeedback@cisco.com

permit sctp (IPv6)

To create an access control list (ACL) rule that permits IPv6 sctp traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

General Syntax

```
[sequence-number] permit sctp source [operator port [port] | portgroup portgroup] destination
[operator port [port] | portgroup portgroup] [dscp dscp | flow-label flow-label-value |
fragments | log]
```

```
no permit sctp source [operator port [port] | portgroup portgroup] destination [operator port
[port] | portgroup portgroup] [dscp dscp | flow-label flow-label-value | fragments | log]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “Source and Destination” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

<i>operator port [port]</i>	<p>(Optional) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the <i>operator</i> and <i>port</i> arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>The <i>port</i> 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.</p> <p>A second <i>port</i> argument is required only when the <i>operator</i> argument is a range.</p> <p>The <i>operator</i> argument must be one of the following keywords:</p> <ul style="list-style-type: none"> • eq—Matches only if the port in the packet is equal to the <i>port</i> argument. • gt—Matches only if the port in the packet is greater than the <i>port</i> argument. • lt—Matches only if the port in the packet is less than the <i>port</i> argument. • neq—Matches only if the port in the packet is not equal to the <i>port</i> argument. • range—Requires two <i>port</i> arguments and matches only if the port in the packet is equal to or greater than the first <i>port</i> argument and equal to or less than the second <i>port</i> argument.
portgroup <i>portgroup</i>	<p>(Optional) 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 <i>portgroup</i> argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>Use the object-group ip port command to create and change IP port-group objects.</p>

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only 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)
flow-label <i>flow-label-value</i>	<p>(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the <i>flow-label-value</i> argument. The <i>flow-label-value</i> argument can be an integer from 0 to 1048575.</p>

Send comments to nexus5k-docfeedback@cisco.com

fragments	(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. 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 devices requires to evaluate those options is contained only in initial fragments.
log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable

Command Default None

Command Modes IPv6 ACL configuration mode

Command History	Release	Modification
	5.2(1)N1(1)	Added ACL logging capability.
	4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions 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.

Source and Destination

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

- Address and variable-length subnet mask—You can use an IPv6 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:

IPv6-address/prefix-len

This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

```
switch(config-acl)# permit sctp 2001:0db8:85a3::/48 any
```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

host *IPv6-address*

Send comments to nexus5k-docfeedback@cisco.com

This syntax is equivalent to *IPv6-address/128*.

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-acl)# permit sctp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 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.

Examples

This example shows how to configure an IPv6 ACL named `acl-lab13-ipv6` with rules permitting all SCTP traffic from the 2001:0db8:85a3:: and 2001:0db8:69f2:: networks to the 2001:0db8:be03:2112:: network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# permit sctp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit sctp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

This example shows how to configure an IPv6 ACL named `ipv6-eng-to-marketing` with a rule that permits all IPv6 traffic from an IPv6-address object group named `eng_ipv6` to an IPv6-address object group named `marketing_group`:

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# permit sctp addrgroup eng_ipv6 addrgroup marketing_group
```

Related Commands

Command	Description
deny (IPv6)	Configures a deny rule in an IPv6 ACL.
ipv6 access-list	Configures an IPv6 ACL.
remark	Configures a remark in an ACL.

Send comments to nexus5k-docfeedback@cisco.com

permit tcp (IPv6)

To create an access control list (ACL) rule that permits IPv6 TCP traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

```
[sequence-number] permit tcp source [operator port [port] | portgroup portgroup] destination
[operator port [port] | portgroup portgroup] [dscp dscp | flags | flow-label flow-label-value |
fragments | log | established]
```

```
no permit tcp source [operator port [port] | portgroup portgroup] destination [operator port [port]
| portgroup portgroup] [dscp dscp | flags | flow-label flow-label-value | fragments | log |
established]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

<i>operator port [port]</i>	<p>(Optional) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the <i>operator</i> and <i>port</i> arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>The <i>port</i> argument can be the name or the number of a TCP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see the “TCP Port Names” section in the “Usage Guidelines” section.</p> <p>A second <i>port</i> argument is required only when the <i>operator</i> argument is a range.</p> <p>The <i>operator</i> argument must be one of the following keywords:</p> <ul style="list-style-type: none"> • eq—Matches only if the port in the packet is equal to the <i>port</i> argument. • gt—Matches only if the port in the packet is greater than the <i>port</i> argument. • lt—Matches only if the port in the packet is less than the <i>port</i> argument. • neq—Matches only if the port in the packet is not equal to the <i>port</i> argument. • range—Requires two <i>port</i> arguments and matches only if the port in the packet is equal to or greater than the first <i>port</i> argument and equal to or less than the second <i>port</i> argument.
portgroup <i>portgroup</i>	<p>(Optional) 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 <i>portgroup</i> argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>Use the object-group ip port command to create and change IP port-group objects.</p>

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only 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)
established	<p>(Optional) Specifies that the rule matches only packets that belong to an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection.</p>
flags	<p>(Optional) Rule matches only packets that have specific TCP control bit flags set. The value of the <i>flags</i> argument must be one or more of the following keywords:</p> <ul style="list-style-type: none"> ack fin psh rst syn urg

Send comments to nexus5k-docfeedback@cisco.com

flow-label <i>flow-label-value</i>	(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the <i>flow-label-value</i> argument. The <i>flow-label-value</i> argument can be an integer from 0 to 1048575.
fragments	(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. 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 devices requires to evaluate those options is contained only in initial fragments.
log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable

Command Default	None
------------------------	------

Command Modes	IPv6 ACL configuration mode
----------------------	-----------------------------

Command History	Release	Modification
	5.2(1)N1(1)	Added ACL logging capability.
	4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions 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.

Source and Destination

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

- Address and variable-length subnet mask—You can use an IPv6 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:

IPv6-address/prefix-len

This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

```
switch(config-acl)# permit tcp 2001:0db8:85a3::/48 any
```

Send comments to nexus5k-docfeedback@cisco.com

- **Host address**—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

host *IPv6-address*

This syntax is equivalent to *IPv6-address/128*.

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-acl)# permit tcp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- **Any address**—You can use the **any** keyword to specify that a source or destination is any IPv6 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.

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)
- **nnntp**—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)

Send comments to nexus5k-docfeedback@cisco.com

- **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)

Examples

This example shows how to configure an IPv6 ACL named `acl-lab13-ipv6` with rules permitting all TCP traffic from the `2001:0db8:85a3::` and `2001:0db8:69f2::` networks to the `2001:0db8:be03:2112::` network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

This example shows how to configure an IPv6 ACL named `ipv6-eng-to-marketing` with a rule that permits all IPv6 TCP traffic from an IPv6-address object group named `eng_ipv6` to an IPv6-address object group named `marketing_group`:

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# permit tcp addrgroup eng_ipv6 addrgroup marketing_group
```

Related Commands

Command	Description
deny (IPv6)	Configures a deny rule in an IPv6 ACL.
ipv6 access-list	Configures an IPv6 ACL.
remark	Configures a remark in an ACL.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

permit udp (IPv6)

To create an access control list (ACL) rule that permits IPv6 UDP traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

General Syntax

```
[sequence-number] permit udp source [operator port [port] | portgroup portgroup] destination
[operator port [port] | portgroup portgroup] [dscp dscp | flow-label flow-label-value |
fragments | log]
```

```
no permit udp source [operator port [port] | portgroup portgroup] destination [operator port
[port] | portgroup portgroup] [dscp dscp | flow-label flow-label-value | fragments | log]
```

```
no sequence-number
```

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.
<i>destination</i>	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the “ Source and Destination ” section in the “Usage Guidelines” section.

Send comments to nexus5k-docfeedback@cisco.com

<i>operator port [port]</i>	<p>(Optional) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the <i>operator</i> and <i>port</i> arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>The <i>port</i> argument can be the name or the number of a UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see the “UDP Port Names” section in the “Usage Guidelines” section.</p> <p>A second <i>port</i> argument is required only when the <i>operator</i> argument is a range.</p> <p>The <i>operator</i> argument must be one of the following keywords:</p> <ul style="list-style-type: none"> • eq—Matches only if the port in the packet is equal to the <i>port</i> argument. • gt—Matches only if the port in the packet is greater than the <i>port</i> argument. • lt—Matches only if the port in the packet is less than the <i>port</i> argument. • neq—Matches only if the port in the packet is not equal to the <i>port</i> argument. • range—Requires two <i>port</i> arguments and matches only if the port in the packet is equal to or greater than the first <i>port</i> argument and equal to or less than the second <i>port</i> argument.
portgroup <i>portgroup</i>	<p>(Optional) 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 <i>portgroup</i> argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>Use the object-group ip port command to create and change IP port-group objects.</p>

Send comments to nexus5k-docfeedback@cisco.com

dscp <i>dscp</i>	<p>(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"> 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only 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)
flow-label <i>flow-label-value</i>	<p>(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the <i>flow-label-value</i> argument. The <i>flow-label-value</i> argument can be an integer from 0 to 1048575.</p>

Send comments to nexus5k-docfeedback@cisco.com

fragments	(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. 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 devices requires to evaluate those options is contained only in initial fragments.
log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: <ul style="list-style-type: none"> • Protocol • Source and destination addresses • Source and destination port numbers, if applicable

Command Default	None
------------------------	------

Command Modes	IPv6 ACL configuration mode
----------------------	-----------------------------

Command History	Release	Modification
	5.2(1)N1(1)	Added ACL logging capability.
	4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions 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.

Source and Destination

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

- Address and variable-length subnet mask—You can use an IPv6 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:

IPv6-address/prefix-len

This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

```
switch(config-acl)# permit udp 2001:0db8:85a3::/48 any
```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

host *IPv6-address*

Send comments to nexus5k-docfeedback@cisco.com

This syntax is equivalent to *IPv6-address/128*.

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-acl)# permit udp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 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.

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)
- **xmcp**—X Display Manager Control Protocol (177)

Send comments to nexus5k-docfeedback@cisco.com

Examples

This example shows how to configure an IPv6 ACL named `acl-lab13-ipv6` with rules permitting all UDP traffic from the `2001:0db8:85a3::` and `2001:0db8:69f2::` networks to the `2001:0db8:be03:2112::` network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

This example shows how to configure an IPv6 ACL named `ipv6-eng-to-marketing` with a rule that permits all UDP traffic from an IPv6-address object group named `eng_ipv6` to an IPv6-address object group named `marketing_group`:

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# permit udp addrgroup eng_ipv6 addrgroup marketing_group
```

Related Commands

Command	Description
deny (IPv6)	Configures a deny rule in an IPv6 ACL.
ipv6 access-list	Configures an IPv6 ACL.
remark	Configures a remark in an ACL.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

permit (MAC)

To create a MAC 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.

[sequence-number] **permit** *source destination [protocol] [cos cos-value] [vlan vlan-id]*

no permit *source destination [protocol] [cos cos-value] [vlan vlan-id]*

no *sequence-number*

Syntax Description

<i>sequence-number</i>	(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.
<i>source</i>	Source MAC 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.
<i>destination</i>	Destination MAC 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.
<i>protocol</i>	(Optional) Protocol number that the rule matches. Valid protocol numbers are 0x0 to 0xffff. For listings of valid protocol names, see “MAC Protocols” in the “Usage Guidelines” section.
cos <i>cos-value</i>	(Optional) Specifies that the rule matches only packets whose IEEE 802.1Q header contains the Class of Service (CoS) value given in the <i>cos-value</i> argument. The <i>cos-value</i> argument can be an integer from 0 to 7.
vlan <i>vlan-id</i>	(Optional) Specifies that the rule matches only packets whose IEEE 802.1Q header contains the VLAN ID given. The <i>vlan-id</i> argument can be an integer from 1 to 4094.

Command Default

A newly created MAC 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.

Command Modes

MAC ACL configuration mode

Send comments to nexus5k-docfeedback@cisco.com

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

When the switch applies a MAC 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 two ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and mask—You can use a MAC address followed by a mask to specify a single address or a group of addresses. The syntax is as follows:

MAC-address MAC-mask

This example specifies the *source* argument with the MAC address 00c0.4f03.0a72:

```
switch(config-acl)# permit 00c0.4f03.0a72 0000.0000.0000 any
```

This example specifies the *destination* argument with a MAC address for all hosts with a MAC vendor code of 00603e:

```
switch(config-acl)# permit any 0060.3e00.0000 0000.0000.0000
```

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

MAC Protocols

The *protocol* argument can be the MAC protocol number or a keyword. The protocol number is a four-byte hexadecimal number prefixed with 0x. Valid protocol numbers are from 0x0 to 0xffff. Valid keywords are the following:

- aarp**—Appletalk ARP (0x80f3)
- appletalk**—Appletalk (0x809b)
- decnet-iv**—DECnet Phase IV (0x6003)
- diagnostic**—DEC Diagnostic Protocol (0x6005)
- etype-6000**—Ethernet 0x6000 (0x6000)
- etype-8042**—Ethernet 0x8042 (0x8042)
- ip**—Internet Protocol v4 (0x0800)
- lat**—DEC LAT (0x6004)
- lvc-sca**—DEC LAVC, SCA (0x6007)
- mop-console**—DEC MOP Remote console (0x6002)
- mop-dump**—DEC MOP dump (0x6001)
- vines-echo**—VINES Echo (0x0baf)

Send comments to nexus5k-docfeedback@cisco.com**Examples**

This example shows how to configure a MAC ACL named mac-ip-filter with a rule that permits all IPv4 traffic between two groups of MAC addresses:

```
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
switch(config-mac-acl)#
```

Related Commands

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

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	<i>interface-list</i>	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
	4.0(0)N1(1a)	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(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/2 - 8
```

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

```
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
```

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

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

Related Commands	Command	Description
	interface policy deny	Enters interface policy configuration mode for a user role.

Send comments to nexus5k-docfeedback@cisco.com

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

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	<i>vlan-list</i>	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
	4.0(0)N1(1a)	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(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1-8
```

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

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

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

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

Send comments to nexus5k-docfeedback@cisco.com

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	<i>vrf-list</i>	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
	4.0(0)N1(1a)	This command was introduced.

Examples	<p>This example shows how to configure a range of VRFs for a user role VRF policy:</p> <pre>switch(config)# role name MyRole switch(config-role)# vrf policy deny switch(config-role-vrf)# permit vrf management</pre>
-----------------	---

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.

Send comments to nexus5k-docfeedback@cisco.com

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	<i>vsan-list</i> Range of VSANs accessible to a user role. The range is from 1 to 4093. You can separate the range using the following separators: <ul style="list-style-type: none">, 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
	4.0(0)N1(1a)	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: <pre>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)#</pre>	
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.

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com



R Commands

This chapter describes the Cisco NX-OS security commands that begin with R.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

radius-server deadtime

To configure the dead-time interval for all RADIUS servers on a Cisco Nexus 5000 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	<i>minutes</i>	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
	4.0(0)N1(1a)	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(config)# radius-server deadtime 5
```

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(config)# no radius-server deadtime 5
```

Related Commands	Command	Description
	show radius-server	Displays RADIUS server information.

Send comments to nexus5k-docfeedback@cisco.com

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
4.0(0)N1(1a)	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(config)# radius-server directed-request
```

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

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

Related Commands

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

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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 | 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]]
```

Syntax Description

<i>hostname</i>	RADIUS server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
<i>ipv4-address</i>	RADIUS server IPv4 address in the <i>A.B.C.D</i> format.
<i>ipv6-address</i>	RADIUS server IPv6 address in the <i>X:X:X:X</i> 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.
<i>shared-secret</i>	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 <i>port-number</i>	(Optional) Configures the RADIUS server port for accounting. The range is from 0 to 65535.
auth-port <i>port-number</i>	(Optional) Configures the RADIUS server port for authentication. The range is from 0 to 65535.
authentication	(Optional) Configures authentication.
retransmit <i>count</i>	(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 <i>time</i>	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes.
password <i>password</i>	Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.

Send comments to nexus5k-docfeedback@cisco.com

username <i>name</i>	Specifies a username in the test packets. The is alphanumeric, not case sensitive, and has a maximum of 32 characters.
timeout <i>seconds</i>	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
4.0(0)N1(1a)	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(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
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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.
	<i>shared-secret</i>	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
	4.0(0)N1(1a)	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(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(config)# radius-server key 7 public pac
```

Related Commands	Command	Description
	show radius-server	Displays RADIUS server information.

Send comments to nexus5k-docfeedback@cisco.com

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	<i>count</i>	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
	4.0(0)N1(1a)	This command was introduced.

Examples	<p>This example shows how to configure the number of retransmissions to RADIUS servers:</p> <pre>switch(config)# radius-server retransmit 3</pre> <p>This example shows how to revert to the default number of retransmissions to RADIUS servers:</p> <pre>switch(config)# no radius-server retransmit 3</pre>
----------	--

Related Commands	Command	Description
	show radius-server	Displays RADIUS server information.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	<i>seconds</i>	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
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to configure the timeout interval:

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

This example shows how to revert to the default interval:

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

Related Commands	Command	Description
	show radius-server	Displays RADIUS server information.

Send comments to nexus5k-docfeedback@cisco.com

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

<i>sequence-number</i>	<p>(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.</p> <p>A sequence number can be any integer between 1 and 4294967295.</p> <p>By default, the first rule in an ACL has a sequence number of 10.</p> <p>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.</p> <p>Use the resequence command to reassign sequence numbers to remarks and rules.</p>
<i>remark</i>	Text of the remark. This argument can be up to 100 characters.

Command Default

No ACL contains a remark by default.

Command Modes

IPv4 ACL configuration mode
MAC ACL configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

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(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
```

Send comments to nexus5k-docfeedback@cisco.com

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.
show access-list	Displays all ACLs or one ACL.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

resequence

To reassign sequence numbers to all rules in an access control list (ACL) or a time range, use the **resequence** command.

resequence [**ip** | **ipv6** | **mac**] **access-list** *access-list-name* *starting-number* *increment*

resequence *time-range* *time-range-name* *starting-number* *increment*

Syntax Description	ip	Type of the ACL.
	ipv6	
	mac	
	access-list <i>access-list-name</i>	Specifies the name of the ACL.
	time-range <i>time-range-name</i>	Specifies the name of the time range.
	<i>starting-number</i>	Sequence number for the first rule in the ACL or time range.
	<i>increment</i>	Number that the switch adds to each subsequent sequence number.

Command Default	None
-----------------	------

Command Modes	Global configuration mode
---------------	---------------------------

Command History	Release	Modification
	5.2(1)N1(1)	IPv6 was added.
	4.0(0)N1(1a)	This command was introduced.

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(config)# show ip access-lists ip-acl-01
```

Send comments to nexus5k-docfeedback@cisco.com

```
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)#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
ipv6 access-list	Configures an IPv6 ACL.
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs or a specific ACL.

Send comments to nexus5k-docfeedback@cisco.com

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
4.0(0)N1(1a)	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(config)# role feature-group name MyGroup  
switch(config-role-featuregrp)#
```

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

```
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.

Send comments to nexus5k-docfeedback@cisco.com

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		
	<i>role-name</i>	User role name. The <i>role-name</i> has a maximum length of 16 characters and is a case-sensitive, alphanumeric character string.
	default-role	Specifies the default user role name.
	<i>privilege-role</i>	Privilege user role, which can be one of the following: <ul style="list-style-type: none"> • 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
	4.0(0)N1(1a)	This command was introduced.
	5.0(2)N1(1)	Support for creating privileged role was added.

Send comments to nexus5k-docfeedback@cisco.com

Usage Guidelines

A Cisco Nexus 5000 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(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(config)# role name priv-1  
switch(config-role)#
```

This example shows how to remove a user role:

```
switch(config)# no role name MyRole
```

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

rollback running-config

To rollback a running configuration, use the **rollback running-config** command.

```
rollback running-config { checkpoint checkpoint-name | file { bootflash: |
volatile: } [//server][directory/][filename] [atomic] [verbose] }
```

Syntax Description

checkpoint	Specifies that the running configuration be rolled back to the checkpoint.
<i>checkpoint-name</i>	Checkpoint name. The name can be a maximum of 32 characters.
file	Specifies that the running configuration be rolled back to the configuration file.
bootflash:	Specifies the bootflash local writable storage file system.
volatile:	Specifies the volatile local writable storage file system.
<i>//server</i>	Name of the server. Valid values are <i>///</i> , <i>//module-1/</i> , <i>//sup-1/</i> , <i>//sup-active/</i> , or <i>//sup-local/</i> . The double slash (//) is required.
<i>directory/</i>	Name of a directory. The directory name is case sensitive.
<i>filename</i>	Name of the checkpoint configuration file. The filename is case sensitive.
atomic	(Optional) Specifies that the rollback execution is to stop when the first failure occurs while applying the patch. This is the default mode.
verbose	(Optional) Specifies that the roll back execution steps be displayed during a rollback operation.



Note

There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

Atomic rollback

Command Modes

EXEC mode

Command History

Release	Modification
5.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can roll back to a checkpoint name or file. Before you roll back, you can view the differences between the source and destination checkpoints that reference the current or saved configurations using the **show diff rollback-patch** command.

A rollback to a specified checkpoint restores the active configuration of the system to the checkpointed configuration.

A rollback to files on bootflash is supported only on files that are created using the **checkpoint checkpoint_name** command and not on any other type of ASCII file.

Send comments to nexus5k-docfeedback@cisco.com



Note

If you make a configuration change during an atomic rollback, the rollback will fail. You must manually correct the error and then run the **rollback** command.

Examples

This example shows how to roll back the running configuration to a checkpoint, named chkpnt-1, in verbose mode:

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration-->
switch# checkpoint chkpnt-2
<-- modify configuration in running configuration-->
switch# rollback running-config chkpnt-1 verbose
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Collecting Running-Config
#Generating Rollback Patch
Rollback Patch is Empty

Rollback completed successfully.

switch#
```

This example shows how to roll back the running configuration to a checkpoint configuration file named chkpnt_configSep9-1.txt in the bootflash storage system:

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration-->
switch# checkpoint chkpnt-2
switch# rollback running-config file bootflash:///chkpnt_configSep9-1.txt
switch#
```

Related Commands

Command	Description
rollback	Rolls back the switch to any of the saved checkpoints.
show checkpoint	Displays checkpoint information.
show diff rollback-patch checkpoint	Displays the differences between current checkpoint and saved configuration.
show diff rollback-patch file	Displays the differences between the current checkpoint file and the saved configuration.
show diff rollback-patch running-config	Displays the differences between the current running configuration and the saved checkpoint configuration.

Send comments to nexus5k-docfeedback@cisco.com

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

<i>number</i>	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 <i>command-string</i>	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 <i>feature-name</i>	(Optional) Specifies a feature name. Use the show role feature command to list the switch feature names.
feature-group <i>group-name</i>	(Optional) Specifies a feature group.

Command Default

None

Command Modes

User role configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
5.0(2)N1(1)	Deny rules can be added to a privilege 0 (priv-0) role.

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(config)# role name MyRole
switch(config-role)# rule 1 deny command clear users
```

Send comments to nexus5k-docfeedback@cisco.com

```
switch(config-role)# rule 1 permit read-write feature-group L3
```

This example shows how to add rules to a user role with privilege 0:

```
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(config)# role MyRole
switch(config-role)# no rule 10
```

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.

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com



S Commands

This chapter describes the Cisco NX-OS security commands that begin with S.

Send comments to nexus5k-docfeedback@cisco.com

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* | *ipv6-address* | *hostname*}

no server {*ipv4-address* | *ipv6-address* | *hostname*}

Syntax Description

<i>ipv4-address</i>	Server IPv4 address in the <i>A.B.C.D</i> format.
<i>ipv6-address</i>	Server IPv6 address in the <i>X:X:X::X</i> format.
<i>hostname</i>	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
4.0(0)N1(1a)	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(config)# aaa group server radius RadServer
switch(config-radius)# server 192.168.1.1
```

This example shows how to delete a server from a RADIUS server group:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# no server 192.168.1.1
```

This example shows how to add a server to a TACACS+ server group:

```
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
```

Send comments to nexus5k-docfeedback@cisco.com

```
switch(config-tacacs+)# server 192.168.2.2
```

This example shows how to delete a server from a TACACS+ server group:

```
switch(config)# feature tacacs+  
switch(config)# aaa group server tacacs+ TacServer  
switch(config-tacacs+)# no server 192.168.2.2
```

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.

Send comments to nexus5k-docfeedback@cisco.com

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

<i>username</i>	(Optional) Username for the SSH session. The username is not case sensitive and has a maximum of 64 characters.
<i>ipv4-address</i>	IPv4 address of the remote host.
<i>hostname</i>	Hostname of the remote host. The hostname is case sensitive and has a maximum of 64 characters.
vrf <i>vrf-name</i>	(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
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The switch supports SSH version 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.

Send comments to nexus5k-docfeedback@cisco.com

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		
<i>username</i>	(Optional) Username for the SSH session. The username is not case sensitive and has a maximum of 64 characters.	
<i>ipv6-address</i>	IPv6 address of the remote host.	
<i>hostname</i>	Hostname of the remote host. The hostname is case sensitive and has a maximum of 64 characters.	
vrf <i>vrf-name</i>	(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
	4.0(1a)N1(1)	This command was introduced.

Usage Guidelines	The switch supports SSH version 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.

Send comments to nexus5k-docfeedback@cisco.com

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
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software supports SSH version 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(config)# ssh key rsa
```

This example shows how to create an SSH server key using RSA with a specified key length:

```
switch(config)# ssh key rsa 768
```

This example shows how to replace an SSH server key using DSA with the force option:

```
switch(config)# no ssh server enable
switch(config)# ssh key dsa force
switch(config)# ssh server enable
```

This example shows how to remove the DSA SSH server key:

```
switch(config)# no ssh server enable
switch(config)# no ssh key dsa
```

Send comments to nexus5k-docfeedback@cisco.com

```
switch(config)# ssh server enable
```

This example shows how to remove all SSH server keys:

```
switch(config)# no ssh server enable  
switch(config)# no ssh key  
switch(config)# ssh server enable
```

Related Commands

Command	Description
show ssh key	Displays the SSH server key information.
ssh server enable	Enables the SSH server.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

ssh login-attempts

To configure the maximum number of times that a user can attempt to log in to a Secure Shell (SSH) session, use the **ssh login-attempts** command. To disable the configuration, use the **no** form of this command.

ssh login-attempts *number*

no ssh login-attempts *number*

Syntax Description	<i>number</i> Maximum number of login attempts. The range is from 1 to 10.					
Command Default	3					
Command Modes	Global configuration					
SupportedUserRoles	network-admin vdc-admin					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.0(2)</td><td>This command was introduced</td></tr></table>		Release	Modification	5.0(2)	This command was introduced
Release	Modification					
5.0(2)	This command was introduced					
Usage Guidelines	<p>The total number of login attempts includes attempts through public-key authentication, certificate-based authentication, and password-based authentication.</p> <p>This command does not require a license.</p> <p>If the user exceeds the maximum number of permitted login attempts, the session disconnects.</p>					
Examples	<p>This example shows how to configure the maximum number of times that a user can attempt to log in to an SSH session:</p> <pre>switch# configure terminal switch(config)# ssh login-attempts 5</pre> <p>This example shows how to disable the SSH login attempt configuration:</p> <pre>switch# configure terminal switch(config)# no ssh login-attempts</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show running-config security all</td><td>Displays the configured maximum number of SSH login attempts.</td></tr></table>		Command	Description	show running-config security all	Displays the configured maximum number of SSH login attempts.
Command	Description					
show running-config security all	Displays the configured maximum number of SSH login attempts.					

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	This command was introduced.

Usage Guidelines	The switch supports SSH version 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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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 <i>percentage</i>	Specifies the percentage of the suppression level. The range is from 0 to 100 percent.
<i>fraction</i>	(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
4.0(0)N1(1a)	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(config-if)# storm-control broadcast level 30
```

Send comments to nexus5k-docfeedback@cisco.com

This example shows how to disable the suppression mode for multicast traffic:

```
switch(config-if)# no storm-control multicast level
```

Related Commands

Command	Description
show interface	Displays the storm-control suppression counters for an interface.
show running-config	Displays the configuration of the interface.

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com



Show Commands

This chapter describes the Cisco NX-OS security **show** commands.

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to display the configuration of the accounting log:

```
switch# show aaa accounting
      default: local
switch#
```

Related Commands	Command	Description
	aaa accounting default	Configures AAA methods for accounting.

Send comments to nexus5k-docfeedback@cisco.com

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	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
	4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the configured authentication parameters:

```
switch# show aaa authentication
      default: group t1
      console: group t1
switch#
```

This example shows how to display the authentication login error enable configuration:

```
switch# show aaa authentication login error-enable
disabled
switch#
```

This example shows how to display the authentication login MS-CHAP configuration:

```
switch# show aaa authentication login mschap
MSCHAP is disabled
switch#
```

Related Commands	Command	Description
	aaa authentication	Configures AAA authentication methods.

Send comments to nexus5k-docfeedback@cisco.com

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
	4.2(1)N1(1)	This command was introduced.

Examples	<p>This example shows how to display the configured authorization methods:</p> <pre>switch# show aaa authorization AAA command authorization: default authorization for config-commands: none switch#</pre>
-----------------	---

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.

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	This command was introduced.

Examples	This example shows how to display AAA group information:
-----------------	--

```
switch# show aaa groups
radius
t1
tacacs
rad1
switch#
```

Related Commands	Command	Description
	aaa group server radius	Creates a RADIUS server group.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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
	4.0(0)N1(1a)	This command was introduced.
Examples	<p>This example shows how to display the status of the default role assigned by the AAA server administrator for remote authentication:</p> <pre>switch# show aaa user default-role enabled switch#</pre>	
Related Commands	Command	Description
	aaa user default-role	Configures the default user for remote authentication.
	show aaa authentication	Displays AAA authentication information.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	<i>access-list-name</i>	(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 <i>access-list-name</i> argument to specify an ACL.
-----------------	--

Command Modes	EXEC mode
---------------	-----------

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display all IPv4 and MAC ACLs on the switch:

```
switch# show access-lists
```

In Cisco NX-OS Release 5.0(2)N1(1), the following output is displayed:

```
switch# show access-lists
```

```
IP access list BulkData
  10 deny ip any any
IP access list CriticalData
  10 deny ip any any
IP access list Scavenger
  10 deny ip any any
MAC access list acl-mac
  10 permit any any
IP access list denyv4
  20 deny ip 10.10.10.0/24 10.20.10.0/24 fragments
  30 permit udp 10.10.10.0/24 10.20.10.0/24 lt 400
  40 permit icmp any any router-advertisement
  60 deny tcp 10.10.10.0/24 10.20.10.0/24 syn
  70 permit igmp any any host-report
  80 deny tcp any any rst
  90 deny tcp any any ack
  100 permit tcp any any fin
  110 permit tcp any gt 300 any lt 400
  130 deny tcp any range 200 300 any lt 600
  140 deny tcp any range 200 300 any lt 600
IP access list dot
  statistics per-entry
  10 permit ip 20.1.1.1 255.255.255.0 20.10.1.1 255.255.255.0 precedence f
lash-override
  20 deny ip 20.1.1.1/24 20.10.1.1/24 fragments
  30 permit tcp any any fragments
```

Send comments to nexus5k-docfeedback@cisco.com

```

    40 deny tcp any eq 400 any eq 500
IP access list ipPacl
    statistics per-entry
    10 deny tcp any eq 400 any eq 500
IP access list ipv4
    10 permit ip 10.10.10.1 225.255.255.0 any fragments
    20 permit ip any any dscp ef
IP access list ipv4Acl
    10 permit ip 10.10.10.1/32 10.10.10.2/32
MAC access list test
    statistics per-entry
    10 deny 0000.1111.2222 0000.0000.0000 0000.1111.3333 ffff.0000.0000
IP access list voice
    10 remark - avaya rtp range
    20 permit udp any range 49072 50175 any range 49072 50175 dscp ef
    30 permit udp any range 49072 50175 any range 50176 50353 dscp ef
    40 permit udp any range 50176 50353 any range 49072 50175 dscp ef
    50 permit udp any range 50176 50353 any range 50176 50353 dscp ef
    60 permit udp any range 2048 2815 any range 2048 2815 dscp ef
    70 permit udp any range 2048 2815 any range 2816 3028 dscp ef
    80 permit udp any range 2816 3028 any range 2816 3028 dscp ef
    90 permit udp any range 2816 3028 any range 2048 2815 dscp ef
    100 remark -- cisco rtp range
switch#

```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

show accounting log

To display the accounting log contents, use the **show accounting log** command.

show accounting log [*size*] [**start-time** *year month day HH:MM:SS*] [**end-time** *year month day HH:MM:SS*]

Syntax Description	<i>size</i>	(Optional) Amount of the log to display in bytes. The range is from 0 to 250000.
	start-time <i>year month day HH:MM:SS</i>	(Optional) Specifies a start time. The <i>year</i> argument is in yyyy format. The <i>month</i> is the three-letter English abbreviation. The <i>day</i> argument range is from 1 to 31. The <i>HH:MM:SS</i> argument is in standard 24-hour format.
	end-time <i>year month day HH:MM:SS</i>	(Optional) Specifies an end time. The <i>year</i> argument is in yyyy format. The <i>month</i> is the three-letter English abbreviation. The <i>day</i> argument range is from 1 to 31. The <i>HH:MM:SS</i> argument is in standard 24-hour format.

Command Default	None
------------------------	------

Command Modes	EXEC mode
----------------------	-----------

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display the entire accounting log:

```
switch# show accounting log
```

In Cisco NX-OS Release, this command displays the following output:

```
switch# show accounting log
```

```
Mon Aug 16 09:37:43 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; interface vfc3 ; bind interface Ethernet1/12 (SUCCESS)
Mon Aug 16 09:38:20 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; interface vfc3 ; no shutdown (REDIRECT)
Mon Aug 16 09:38:20 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=Interface vfc3 state updated to up
Mon Aug 16 09:38:20 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; interface vfc3 ; no shutdown (SUCCESS)
Mon Aug 16 09:38:20 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; interface vfc3 ; no shutdown (SUCCESS)
Mon Aug 16 09:48:05 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; interface Ethernet2/1 (SUCCESS)
Mon Aug 16 09:55:27 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; vtp mode client (FAILURE)
Mon Aug 16 09:55:35 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; vtp mode server (FAILURE)
Mon Aug 16 10:03:46 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; no vtp mode (FAILURE)
```

Send comments to nexus5k-docfeedback@cisco.com

```
Mon Aug 16 10:04:11 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; vtp mode transparent (SUCCESS)
Mon Aug 16 10:04:20 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; vtp domain MyDomain (SUCCESS)
Mon Aug 16 10:04:39 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; vtp password MyPass (SUCCESS)
Mon Aug 16 10:05:17 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; no vtp password (SUCCESS)
Mon Aug 16 10:06:46 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; vtp pruning (SUCCESS)
Mon Aug 16 10:09:11 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=configure terminal ; interface Ethernet1/12 (SUCCESS)
Mon Aug 16 10:32:33 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=clear vtp counters (SUCCESS)
Mon Aug 16 10:35:20 2010:type=stop:id=72.163.177.184@pts/0:user=admin:cmd=shell terminated because of telnet closed
--More--
switch#
```

This example shows how to display 400 bytes of the accounting log:

```
switch# show accounting log 400
```

This example shows how to display the accounting log starting at 16:00:00 on February 16, 2008:

```
switch# show accounting log start-time 2008 Feb 16 16:00:00
```

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	<i>access-list-name</i> (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
	5.1(3)N1(1)	This command was introduced.

Usage Guidelines



Note

As of Cisco NX-OS Release 5.1(3)N1(1), an ARP access list is supported only for Control Plane Policing (CoPP).

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
```

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.

Send comments to nexus5k-docfeedback@cisco.com

show checkpoint

To display the configuration at the time a checkpoint was implemented, use the **show checkpoint** command.

show checkpoint [*checkpoint-name*] [**all** [**system** | **user**]]

Syntax Description	
<i>checkpoint-name</i>	(Optional) Checkpoint name. The name can be a maximum of 32 characters.
all	(Optional) Displays user-configured and system-configured checkpoints.
system	(Optional) Displays all system-configured checkpoints.
user	(Optional) Displays all user-configured checkpoints.

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	5.0(2)N1(1)	This command was introduced.

Usage Guidelines The command output displays a history of the most recent (up to ten) checkpoint IDs. The checkpoint IDs represent the rollback points that allow the user to restore the system to a checkpoint configuration.

Examples This example shows how to display the rollback checkpoints configured in the local switch:

```
switch# show checkpoint
-----
Name: chkpnt-1

!Command: Checkpoint cmd vdc 1
!Time: Mon Sep  6 09:40:47 2010

version 5.0(2)N1(1)
feature telnet
feature tacacs+
cfs eth distribute
feature private-vlan
feature udld
feature interface-vlan
feature lacp
feature vpc
feature lldp
feature fex

username adminbackup password 5 ! role network-operator
username admin password 5 $1$KIPRDtFF$7eUMjCA7Nkhktzebsg5/0 role network-admin
```

Send comments to nexus5k-docfeedback@cisco.com

```
no password strength-check
ip domain-lookup
ip domain-lookup
hostname switch
ip access-list ipl
class-map type qos class-fcoe
  match cos 4
class-map type qos match-all cq1
  match cos 4
  match precedence 7
class-map type qos match-all cq2
  match cos 5
  match dscp 10
class-map type qos match-any cq3
  match precedence 7

<--output truncated-->
switch#
```

This example shows how to display information about a specific checkpoint:

```
switch# show checkpoint chkpnt-1
```

```
-----
Name: chkpnt-1
```

```
!Command: Checkpoint cmd vdc 1
!Time: Mon Sep  6 09:40:47 2010
```

```
version 5.0(2)N1(1)
feature telnet
feature tacacs+
cfs eth distribute
feature private-vlan
feature udld
feature interface-vlan
feature lacp
feature vpc
feature lldp
feature fex
```

```
username adminbackup password 5 ! role network-operator
username admin password 5 $1$KIPRDtFF$7eUMjCAd7Nkhktzebsg5/0 role network-admin
no password strength-check
ip domain-lookup
ip domain-lookup
hostname switch
ip access-list ipl
class-map type qos class-fcoe
  match cos 4
class-map type qos match-all cq1
  match cos 4
  match precedence 7
--More--
switch#
```

This example shows how to display all configured rollback checkpoints:

```
switch# show checkpoint all
```

Send comments to nexus5k-docfeedback@cisco.com

Related Commands	Command	Description
	checkpoint	Creates a checkpoint.
	rollback	Rolls back the configuration to any of the saved checkpoints.
	show checkpoint summary	Displays configuration rollback checkpoints summary.
	show checkpoint system	Displays system-defined rollback checkpoints.
	show checkpoint user	Displays user-configured rollback checkpoints.

Send comments to nexus5k-docfeedback@cisco.com

show checkpoint summary

To display a summary of the configured checkpoints, use the **show checkpoint summary** command.

show checkpoint summary [system | user]

Syntax Description	system	(Optional) Displays a summary of the system-configured checkpoints.
	user	(Optional) Displays a summary of the user-configured checkpoints.

Command Default	None
------------------------	------

Command Modes	EXEC mode
----------------------	-----------

Command History	Release	Modification
	5.0(2)N1(1)	This command was introduced.

Examples This example shows how to display the configuration rollback checkpoints summary:

```
switch# show checkpoint summary
User Checkpoint Summary
User Checkpoint Summary
-----
1) chkpnt-1:
Created by admin
Created at Tue, 08:10:23 14 Sep 2010
Size is 21,508 bytes
Description: Checkpoint to save current configuration, Sep 9 10:02 A.M.

2) chkpnt-2:
Created by admin
Created at Tue, 08:11:46 14 Sep 2010
Size is 21,536 bytes
Description: None

3) user-checkpoint-4:
Created by admin
Created at Tue, 08:16:48 14 Sep 2010
Size is 21,526 bytes
Description: None

switch#
```

This example shows how to display the summary of the system-configured rollback checkpoints:

```
switch# show checkpoint summary system
```

This example shows how to display the summary of the user-configured rollback checkpoints:

```
switch# show checkpoint summary user
-----
1) chkpnt-1:
```

Send comments to nexus5k-docfeedback@cisco.com

Created by admin
 Created at Tue, 08:10:23 14 Sep 2010
 Size is 21,508 bytes
 Description: Checkpoint to save current configuration, Sep 9 10:02 A.M.

2) chkpnt-2:
 Created by admin
 Created at Tue, 08:11:46 14 Sep 2010
 Size is 21,536 bytes
 Description: None

3) user-checkpoint-4:
 Created by admin
 Created at Tue, 08:16:48 14 Sep 2010
 Size is 21,526 bytes
 Description: None

switch#

Related Commands

Command	Description
checkpoint	Creates a checkpoint.
rollback	Rolls back the configuration to any of the saved checkpoints.
show checkpoint	Displays rollback checkpoints.
show checkpoint system	Displays system-defined rollback checkpoints.
show checkpoint user	Displays user-configured rollback checkpoints.

Send comments to nexus5k-docfeedback@cisco.com

show checkpoint system

To display only the system-configured checkpoints, use the **show checkpoint system** command.

show checkpoint system

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	EXEC mode
----------------------	-----------

Command History	Release	Modification
	5.0(2)N1(1)	This command was introduced.

Examples	<p>This example shows how to display the rollback checkpoints defined by the system:</p> <pre>switch# show checkpoint system</pre>
-----------------	--

Related Commands	Command	Description
	checkpoint	Creates a checkpoint.
	rollback	Rolls back the configuration to any of the saved checkpoints.
	show checkpoint	Displays rollback checkpoints.
	show checkpoint user	Displays user-configured rollback checkpoints.

Send comments to nexus5k-docfeedback@cisco.com

show checkpoint user

To display only the user-configured checkpoints, use the **show checkpoint user** command.

show checkpoint user

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	EXEC mode
----------------------	-----------

Command History	Release	Modification
	5.0(2)N1(1)	This command was introduced.

Examples	This example shows how to display the rollback checkpoints configured by the current user:
-----------------	--

```
switch# show checkpoint user
```

```
-----
Name: myCheckpoint
```

```
!Command: Checkpoint cmd vdc 1
!Time: Mon Sep  6 09:40:47 2010
```

```
version 5.0(2)N1(1)
feature telnet
feature tacacs+
cfs eth distribute
feature private-vlan
feature udld
feature interface-vlan
feature lacp
feature vpc
feature lldp
feature fex
```

```
username adminbackup password 5 ! role network-operator
username admin password 5 $1$KIPRDtFF$7eUMjCA7Nkhktzebsg5/0 role network-admin
no password strength-check
ip domain-lookup
ip domain-lookup
hostname switch
ip access-list ip1
class-map type qos class-fcoe
  match cos 4
class-map type qos match-all cq1
  match cos 4
  match precedence 7
```

```
<--output truncated-->
```

Send comments to nexus5k-docfeedback@cisco.com

switch#

Related Commands	Command	Description
	checkpoint	Creates a checkpoint.
	rollback	Rolls back the configuration to any of the saved checkpoints.
	show checkpoint	Displays rollback checkpoints.
	show checkpoint summary	Displays a summary of all configured rollback checkpoints.
	show checkpoint system	Displays system-defined rollback checkpoints.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

show diff rollback-patch checkpoint

To display the configuration differences between two checkpoints, use the **show diff rollback-patch checkpoint** command.

show diff rollback-patch checkpoint *src-checkpoint-name* **checkpoint** *dest-checkpoint-name*

Syntax Description

<i>src-checkpoint-name</i>	Source checkpoint name. The name can be a maximum of 32 characters.
<i>dest-checkpoint-name</i>	Destination checkpoint name. The name can be a maximum of 32 characters.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use this command to view the differences between the source and destination checkpoints that reference current or saved configurations. The configuration differences based on the current running configuration and checkpointed configuration are applied to the system to restore the running state of the system.

Examples

This example shows how to view the changes between two checkpoints, chkpnt-1 and chkpnt-2:

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration-->
switch# checkpoint chkpnt-2
<-- modify configuration in running configuration-->
switch# checkpoint
...
user-checkpoint-4 created Successfully

Done
switch#
<-- modify configuration in running configuration-->
switch# show diff rollback-patch checkpoint user-checkpoint-4 checkpoint chkpnt-1
#Generating Rollback Patch

!!
interface Ethernet1/2
  no untagged cos
  no description Sample config
  exit
!
interface Ethernet1/2
  channel-group 1
```

Send comments to nexus5k-docfeedback@cisco.com

```
!
line vty
switch# rollback chkpnt-1
switch#
```

Related Commands	Command	Description
	checkpoint	Creates a checkpoint.
	rollback	Rolls back the configuration to any of the saved checkpoints.
	show checkpoint	Displays checkpoint information.
	show diff rollback-patch file	Displays the differences between the current checkpoint file and the saved configuration.
	show diff rollback-patch running-config	Displays the differences between the current running configuration and the saved checkpoint configuration.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

show diff rollback-patch file

To display the differences between the two checkpoint configuration files, use the **show diff rollback-patch file** command.

```
show diff rollback-patch file { bootflash: | volatile: } [//server][directory/][src-filename]
{ checkpoint dest-checkpoint-name | file { bootflash: |
volatile: } [//server][directory/][dest-filename] | running-config | startup-config }
```

Syntax Description		
bootflash:		Specifies the bootflash local writable storage file system.
volatile:		Specifies the volatile local writable storage file system.
<i>//server</i>		(Optional) Name of the server. Valid values are <i>///</i> , <i>//module-1/</i> , <i>//sup-1/</i> , <i>//sup-active/</i> , or <i>//sup-local/</i> . The double slash (//) is required.
<i>directory/</i>		(Optional) Name of a directory. The directory name is case sensitive.
<i>src-filename</i>		(Optional) Name of the source checkpoint configuration file. The filename is case sensitive.
<i>dest-filename</i>		(Optional) Name of the destination checkpoint configuration file. The filename is case sensitive.
checkpoint		Specifies a destination checkpoint.
<i>dest-checkpoint-name</i>		Destination checkpoint name. The name can be a maximum of 32 characters.
file		Specifies the destination checkpoint file.
running-config		Specifies that the running configuration be used as the destination.
startup-config		Specifies that the startup configuration be used as the destination.



Note

There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default	None	
Command Modes	EXEC mode	
Command History	Release	Modification
	5.0(2)N1(1)	This command was introduced.

Usage Guidelines	Use this command to view the differences between the source and destination checkpoint configuration files that reference current or saved configurations. The configuration differences based on the current running configuration and checkpointed configuration are applied to the system to restore the running state of the system.
-------------------------	--

Send comments to nexus5k-docfeedback@cisco.com

Examples

This example shows how to view the changes between two checkpoint configurations stored in files in the bootflash storage system:

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration-->
switch# checkpoint chkpnt-2
switch# show diff rollback-patch file bootflash:///chkpnt_configSep9-2.txt file
bootflash:///chkpnt_configSep9-1.txt

switch# rollback file bootflash:///chkpnt_configSep9-1.txt
switch#
```

Related Commands

Command	Description
rollback	Rolls back the switch to any of the saved checkpoints.
show checkpoint	Displays checkpoint information.
show diff rollback-patch checkpoint	Displays the differences between the current checkpoint and the saved configuration.
show diff rollback-patch running-config	Displays the differences between the current running configuration and the saved checkpoint configuration.

[Send comments to nexus5k-docfeedback@cisco.com](#)

show diff rollback-patch running-config

To display the differences between the current running configuration and the saved (checkpointed) configuration, use the **show diff rollback-patch running-config** command.

```
show diff rollback-patch running-config { checkpoint checkpoint-name | file { bootflash: |
volatile: } [//server][directory/][filename] | running-config | startup-config }
```

Syntax Description		
checkpoint		Specifies that the checkpoint be used as the destination in the comparison.
<i>checkpoint-name</i>		Checkpoint name. The name can be a maximum of 32 characters.
file		Specifies that the checkpoint configuration file be used as the destination in the comparison.
bootflash:		Specifies the bootflash local writable storage file system.
volatile:		Specifies the volatile local writable storage file system.
<i>//server</i>		(Optional) Name of the server. Valid values are <i>///</i> , <i>//module-1/</i> , <i>//sup-1/</i> , <i>//sup-active/</i> , or <i>//sup-local/</i> . The double slash (//) is required.
<i>directory/</i>		(Optional) Name of a directory. The directory name is case sensitive.
<i>filename</i>		(Optional) Name of the checkpoint configuration file. The filename is case sensitive.
running-config		Specifies that the running configuration be used as the destination in the comparison.
startup-config		Specifies that the startup configuration be used as the destination in the comparison.



Note

There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	5.0(2)N1(1)	This command was introduced.

Usage Guidelines Use this command to view the differences between the current running configuration and destination checkpoints that reference a saved configuration. The configuration differences based on the current running configuration and checkpointed configuration are applied to the system to restore the running state of the system.

Send comments to nexus5k-docfeedback@cisco.com

Examples

This example shows how to view the configuration changes between the current running configuration and a checkpoint named chkpnt-1:

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration-->
switch# checkpoint chkpnt-2
<-- modify configuration in running configuration-->
switch# show diff rollback-patch running-config checkpoint chkpnt-1
Collecting Running-Config
#Generating Rollback Patch

!!
interface Ethernet1/2
  no description Sample config
  exit
switch#
```

This example shows how to view the configuration changes between the current running configuration and a saved configuration in the bootflash storage system:

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration-->
switch# show diff rollback-patch running-config file chkpnt_configSep9-1.txt
```

This example shows how to view the configuration changes between the current running configuration and a checkpointed running configuration:

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration-->
switch# show diff rollback-patch running-config running-config
```

This example shows how to view the configuration changes between the current running configuration and a saved startup configuration:

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration-->
switch# copy running-config startup-config
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration-->
switch# checkpoint chkpnt-2
switch# show diff rollback-patch running-config startup-config
Collecting Running-Config
Collecting Startup-Config
#Generating Rollback Patch

!!
interface Ethernet1/2
  no untagged cos
  no description Sample config
  exit
password strength-check
no username admin
no username adminbackup
!
```

Send comments to nexus5k-docfeedback@cisco.com

```
interface Ethernet1/2
  channel-group 1
no feature ssh
no feature telnet
switch#
```

Related Commands

Command	Description
rollback	Rolls back the switch to any of the saved checkpoints.
show checkpoint	Displays checkpoint information.
show diff rollback-patch checkpoint	Displays the differences between the current checkpoint and the saved configuration.
show diff rollback-patch file	Displays the differences between the current checkpoint file and the saved configuration.
show diff rollback-patch startup-config	Displays the differences between the current startup configuration and the saved checkpoint configuration.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

show diff rollback-patch startup-config

To display the differences between the current startup configuration and the saved (checkpointed) configuration, use the **show diff rollback-patch startup-config** command.

```
show diff rollback-patch startup-config { checkpoint checkpoint-name | file { bootflash: |
volatile: }[/server][directory/][filename] | running-config | startup-config }
```

Syntax	Description
checkpoint	Specifies that the checkpoint be used as the destination in the comparison.
<i>checkpoint-name</i>	Checkpoint name. The name can be a maximum of 32 characters.
file	Specifies that the checkpoint configuration file be used as the destination in the comparison.
bootflash:	Specifies the bootflash local writable storage file system.
volatile:	Specifies the volatile local writable storage file system.
<i>//server</i>	(Optional) Name of the server. Valid values are <i>///</i> , <i>//module-1/</i> , <i>//sup-1/</i> , <i>//sup-active/</i> , or <i>//sup-local/</i> . The double slash (//) is required.
<i>directory/</i>	(Optional) Name of a directory. The directory name is case sensitive.
<i>filename</i>	(Optional) Name of the checkpoint configuration file. The filename is case sensitive.
running-config	Specifies that the running configuration be used as the destination in the comparison.
startup-config	Specifies that the startup configuration be used as the destination in the comparison.



Note

There can be no spaces in the *filesystem://server/directory/filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	5.0(2)N1(1)	This command was introduced.

Usage Guidelines Use this command to view the differences between the current startup configuration and destination checkpoints that reference a saved configuration. The configuration differences based on the current running configuration and checkpointed configuration are applied to the system to restore the running state of the system.

Send comments to nexus5k-docfeedback@cisco.com

Examples

This example shows how to view the configuration changes between the current startup configuration and a checkpoint named chkpnt-1:

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration-->
switch# checkpoint chkpnt-2
<-- modify configuration in running configuration-->
switch# copy running-config startup-config
switch# show diff rollback-patch startup-config checkpoint chkpnt-1
Collecting Startup-Config
#Generating Rollback Patch

!!
!
feature telnet
feature ssh
username adminbackup password 5 ! role network-operator
username admin password 5 $1$KIPRDtFF$7eUMjCAd7Nkhktzebsg5/0 role network-admin
no password strength-check
switch#
```

This example shows how to view the configuration changes between the current startup configuration and a saved configuration in the bootflash storage system:

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration-->
switch# copy running-config startup-config
switch# show diff rollback-patch startup-config file chkpnt_configSep9-1.txt

switch#
```

This example shows how to view the configuration changes between the current startup configuration and a checkpointed running configuration:

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration-->
switch# copy running-config startup-config
<-- modify configuration in running configuration-->
switch# show diff rollback-patch startup-config running-config
Collecting Running-Config
Collecting Startup-Config
#Generating Rollback Patch

!!
!
feature telnet
feature ssh
username adminbackup password 5 ! role network-operator
username admin password 5 $1$KIPRDtFF$7eUMjCAd7Nkhktzebsg5/0 role network-admin
no password strength-check
switch#
```

This example shows how to view the configuration changes between the current startup configuration and a saved startup configuration:

```
switch# checkpoint chkpnt-1
```

Send comments to nexus5k-docfeedback@cisco.com

```
<-- modify configuration in running configuration-->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration-->
switch# copy running-config startup-config
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration-->
switch# show diff rollback-patch startup-config startup-config
Collecting Startup-Config
#Generating Rollback Patch
Rollback Patch is Empty
switch#
```

Related Commands

Command	Description
rollback	Rolls back the switch to any of the saved checkpoints.
show checkpoint	Displays checkpoint information.
show diff rollback-patch checkpoint	Displays the differences between the current checkpoint and the saved configuration.
show diff rollback-patch file	Displays the differences between the current checkpoint file and the saved configuration.
show diff rollback-patch running-config	Displays the differences between the current running configuration and the saved checkpoint configuration.

Send comments to nexus5k-docfeedback@cisco.com

show http-server

To display information about the HTTP or HTTPS configuration, use the **show http-server** command.

show http-server

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	EXEC mode
----------------------	-----------

Command History	Release	Modification
	5.0(2)N1(1)	This command was introduced.

Usage Guidelines	In releases earlier than Cisco NX-OS Release 5.0(2)N1(1), HTTP or HTTPS is enabled on the switch by default.
-------------------------	--

Examples	This example shows how to display the status of the HTTP server:
-----------------	--

```
switch# show http-server
http-server enabled
switch#
```

Related Commands	Command	Description
	feature http-server	Enables or disables the HTTP or HTTPS server on the switch.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	<i>access-list-name</i>	(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 <i>access-list-name</i> argument to specify an ACL.
-----------------	---

Command Modes	EXEC mode
---------------	-----------

Command History	Release	Modification
	4.0(0)N1(1a)	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 an SVI interface or in a QoS class map, then the command does not display any statistics information.
------------------	---

Examples	This example shows how to display all IPv4 ACLs on the switch:
----------	--

```
switch# show ip access-lists
```

In Cisco NX-OS release 5.0(2)N1(1), this example shows how to display all IPv4 ACLs on the switch:

```
switch# show ip access-lists
IP access list BulkData
  10 deny ip any any
IP access list CriticalData
  10 deny ip any any
IP access list Scavenger
  10 deny ip any any
IP access list denyv4
  20 deny ip 10.10.10.0/24 10.20.10.0/24 fragments
  30 permit udp 10.10.10.0/24 10.20.10.0/24 lt 400
  40 permit icmp any any router-advertisement
  60 deny tcp 10.10.10.0/24 10.20.10.0/24 syn
  70 permit igmp any any host-report
  80 deny tcp any any rst
  90 deny tcp any any ack
  100 permit tcp any any fin
  110 permit tcp any gt 300 any lt 400
  130 deny tcp any range 200 300 any lt 600
  140 deny tcp any range 200 300 any lt 600
IP access list dot
```

Send comments to nexus5k-docfeedback@cisco.com

```

        statistics per-entry
        10 permit ip 20.1.1.1 255.255.255.0 20.10.1.1 255.255.255.0 precedence f
lash-override
        20 deny ip 20.1.1.1/24 20.10.1.1/24 fragments
        30 permit tcp any any fragments
        40 deny tcp any eq 400 any eq 500
IP access list ipPacl
        statistics per-entry
        10 deny tcp any eq 400 any eq 500
IP access list ipv4
        10 permit ip 10.10.10.1 225.255.255.0 any fragments
        20 permit ip any any dscp ef
IP access list ipv4Acl
        10 permit ip 10.10.10.1/32 10.10.10.2/32
IP access list voice
--More--
switch#

```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs or a specific ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

show ip arp

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

```
show ip arp [client | [statistics | summary] [ethernet slot/port | loopback intf-num | mgmt
mgmt-intf-num | port-channel channel-num | vlan vlan-id] [fhrp-non-active-learn] [static]
[detail] [vrf {vrf-name | all | default | management}]
```

Syntax Description	
client	(Optional) Displays ARP information for ARP clients.
statistics	(Optional) Display the global ARP statistics on the switch or the ARP statistics for interfaces.
summary	(Optional) Display the ARP adjacency summary information.
ethernet <i>slot/port</i>	(Optional) Displays the ARP information for an Ethernet interface. The slot number is from 1 to 255 and the port number is from 1 to 128.
loopback <i>intf-num</i>	(Optional) Displays the ARP information for a loopback interface. The loopback interface number is from 0 to 1023.
mgmt <i>mgmt-intf-num</i>	(Optional) Displays the ARP information for a management interface. The interface number is 0.
port-channel <i>channel-num</i>	(Optional) Displays the ARP information for an EtherChannel interface. The channel number range is from 1 to 4096.
vlan <i>vlan-id</i>	(Optional) Displays the ARP information for a specified VLAN. The range is from 1 to 4094, except for the VLANs reserved for internal use.
fhrp-non-active-learn	(Optional) Displays the ARP table information learned only due to a request for a nonactive Cisco First Hop Redundancy Protocol (FHRP) address.
static	(Optional) Displays the static ARP entries.
detail	(Optional) Displays the detailed ARP information.
vrf	(Optional) Specifies the virtual routing and forwarding (VRF) to use.
<i>vrf-name</i>	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
	4.2(1)N1(1)	This command was introduced.
	5.1(3)N1(1)	The client , ethernet , fhrp-non-active-learn , loopback , mgmt , port-channel , static , statistics , and summary keywords were added.

Send comments to nexus5k-docfeedback@cisco.com

Usage Guidelines

You must use the **feature interface-vlan** command before you can display the ARP information for VLAN interfaces.

Examples

This example shows how to display the ARP table:

```
switch# show ip arp
```

```
IP ARP Table for context default
Total number of entries: 1
Address      Age      MAC Address  Interface
90.10.10.2   00:03:11  000d.ece7.df7c  Vlan900
switch#
```

This example shows how to display the detailed ARP table:

```
switch# show ip arp detail
```

```
IP ARP Table for context default
Total number of entries: 1
Address      Age      MAC Address  Interface      Physical Interface
90.10.10.2   00:02:55  000d.ece7.df7c  Vlan900        Ethernet1/12
switch#
```

This example shows how to display the ARP table for VLAN 10 and all VRFs:

```
switch# show ip arp vlan 10 vrf all
```

[Table 1](#) describes the fields shown in the above displays.

Field	Description
IP ARP Table	Context in which the ARP table is applied.
Total number of entries	Total number of ARP entries or messages in the ARP table.
Address	IP address of the switch that the ARP table automatically maps to the MAC address of the switch.
Age	Duration since the switch with a MAC address was mapped to the IP address.
MAC Address	MAC address of the switch.
Interface	Switch interface where packets are forwarded.
Physical Interface	Physical interface, which can one of the following: Ethernet, loopback, EtherChannel, management, or VLAN.

Related Commands

Command	Description
clear ip arp	Clears the ARP cache and table.
feature interface-vlan	Enables the creation of VLAN interfaces.
show running-config arp	Displays the running ARP configuration.

Send comments to nexus5k-docfeedback@cisco.com

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)N1(1)	This command was introduced.

Examples	<p>This example shows how to display the status of the DAI configuration:</p> <pre>switch# show ip arp inspection</pre>
-----------------	---

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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 <i>slot/port</i>	(Optional) Specifies that the output is for an Ethernet interface.
port-channel <i>channel-number</i>	(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)N1(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.

Send comments to nexus5k-docfeedback@cisco.com

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)N1(1)	This command was introduced.

Examples	This example shows how to display the DAI log configuration:
-----------------	--

```
switch# show ip arp inspection log

Syslog Buffer Size : 12
Syslog Rate       : 5 entries per 1 seconds
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 running-config dhcp	Displays DHCP snooping configuration, including the DAI configuration.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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 <i>vlan-list</i>	(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)N1(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 <i>vlan</i>	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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	<i>vlan-list</i>	List of VLANs that have the DAI status. The <i>vlan-list</i> 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)N1(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

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

Vlan : 1
-----
Configuration              : Disabled
Operation State             : Inactive
switch#
```

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

show ip arp sync-entries

To display the Address Resolution Protocol (ARP) table information after an ARP table synchronization, use the **show ip arp sync-entries** command.

show ip arp sync-entries [**detail** | **vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description	detail	(Optional) Displays detailed information about the ARP table.
	vrf	(Optional) Displays ARP table information for a virtual routing and forwarding (VRF) instance.
	<i>vrf-name</i>	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
	all	Displays ARP table information for all VRF entries.
	default	Displays ARP table information for the default VRF entry.
	management	Displays ARP table information for the management VRF entry.

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	5.1(3)N1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to display the global ARP statistics on virtual port channels (vPCs):

```
switch# show ip arp sync-entries
```

Related Commands	Command	Description
	ip arp synchronize	Enables ARP synchronization on a vPC domain.
	show running-config arp	Displays the running configuration information for ARP tables.

Send comments to nexus5k-docfeedback@cisco.com

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(2)N2(1)	This command was introduced.

Examples	This example shows how to display general status information about DHCP snooping:
-----------------	---

```
switch# show ip dhcp snooping
DHCP snooping service is enabled
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
1,13
DHCP snooping is operational on the following VLANs:
1
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface                Trusted
-----                -
Ethernet2/3              Yes

switch#
```

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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
<i>IP-address</i>	(Optional) IPv4 address that the bindings shown must include. Valid entries are in dotted-decimal format.
<i>MAC-address</i>	(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(2)N2(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.
-------------------------	---

Send comments to nexus5k-docfeedback@cisco.com

Examples

This example shows how to show all bindings:

```
switch# show ip dhcp snooping binding
MacAddress      IpAddress      LeaseSec  Type      VLAN  Interface
-----
0f:00:60:b3:23:33  10.3.2.2      infinite  static    13    Ethernet2/46
0f:00:60:b3:23:35  10.2.2.2      infinite  static    100   Ethernet2/10
switch#
```

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, including the IP Source Guard configuration.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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(2)N2(1)	This command was introduced.

Examples	This example shows how to display DHCP snooping statistics:
-----------------	---

```
switch# show ip dhcp snooping statistics
Packets processed 61343
Packets received through cfsoe 0
Packets forwarded 0
Packets forwarded on cfsoe 0
Total packets dropped 61343
Packets dropped from untrusted ports 0
Packets dropped due to MAC address check failure 0
Packets dropped due to Option 82 insertion failure 0
Packets dropped due to o/p intf unknown 0
Packets dropped which were unknown 0
Packets dropped due to dhcp relay not enabled 0
Packets dropped due to no binding entry 0
Packets dropped due to interface error/no interface 61343
Packets dropped due to max hops exceeded 0
switch#
```

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

show ipv6 access-lists

To display all IPv6 access control lists (ACLs) or a specific IPv6 ACL, use the **show ipv6 access-lists** command.

show ipv6 access-lists [*access-list-name*] [**expanded** | **summary**]

Syntax Description	<i>access-list-name</i>	(Optional) Name of an IPv6 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
	expanded	(Optional) Specifies that the contents of IPv6 address groups or port groups show rather than the names of object groups only.
	summary	(Optional) Specifies that the command displays information about the ACL rather than the ACL configuration. For more information, see the "Usage Guidelines" section.

Command Default	None
------------------------	------

Command Modes	EXEC mode
----------------------	-----------

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The device shows all IPv6 ACLs, unless you use the *access-list-name* argument to specify an ACL. The **summary** keyword allows you to display information about the ACL rather than the ACL configuration. The information displayed includes the following:

- Whether per-entry statistics is configured for the ACL.
- The number of rules in the ACL configuration. This number does not reflect how many entries the ACL contains when the device applies it to an interface. If a rule in the ACL uses an object group, the number of entries in the ACL when it is applied may be much greater than the number of rules.
- The interfaces that the ACL is applied to.
- The interfaces that the ACL is active on.

The **show ipv6 access-lists** command displays statistics for each entry in an ACL if the following conditions are both true:

- The ACL configuration contains the **statistics per-entry** command.
- The ACL is applied to an interface that is administratively up.

Examples

This example shows how to display all IPv6 ACLs on a switch:

```
switch# show ipv6 access-lists
```

Send comments to nexus5k-docfeedback@cisco.com

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

show ip verify source

To display the IP Source Guard-enabled interfaces and 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 <i>slot/port</i>	(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 <i>channel-number</i>	(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)N1(1)	This command was introduced.

Examples This example shows how to display the IP Source Guard-enabled interfaces and the IP-to-MAC address bindings on the switch:

```
switch# show ip verify source
IP source guard is enabled on the following interfaces:
```

```
-----
      Ethernet1/2
      Ethernet1/5
```

```
IP source guard operational entries:
```

```
-----
Interface      Filter-mode      IP-address      Mac-address      Vlan
-----
Ethernet1/2    inactive-no-snoop-vlan
Ethernet1/5    inactive-no-snoop-vlan
switch#
```

Related Commands	Command	Description
	ip source binding	Creates a static IP source entry for the specified Ethernet interface.

Send comments to nexus5k-docfeedback@cisco.com

Command	Description
ip verify source dhcp-snooping-vlan	Enables IP Source Guard on an interface.
show running-config dhcp	Displays DHCP snooping configuration, including the IP Source Guard configuration.

Send comments to nexus5k-docfeedback@cisco.com

show mac access-lists

To display all Media Access Control (MAC) access control lists (ACLs) or a specific MAC ACL, use the **show mac access-lists** command.

show mac access-lists [*access-list-name*]

Syntax Description	<i>access-list-name</i> (Optional) Name of a MAC ACL, which can be up to 64 alphanumeric, case-sensitive characters.
--------------------	--

Command Default	The switch shows all MAC ACLs unless you use the <i>access-list-name</i> argument to specify an ACL.
-----------------	--

Command Modes	EXEC mode
---------------	-----------

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Examples	<p>This example shows how to display all MAC ACLs on the switch:</p> <pre>switch# show mac access-lists MAC access list acl-mac 10 permit any any MAC access list test statistics per-entry 10 deny 0000.1111.2222 0000.0000.0000 0000.1111.3333 ffff.0000.0000 switch#</pre>
----------	--

Related Commands	Command	Description
	mac access-list	Configures a MAC ACL.
	show access-lists	Displays all ACLs or a specific ACL.
	show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.

Send comments to nexus5k-docfeedback@cisco.com

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(2)N1(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
User name: admin
Current privilege level: -1
Feature privilege: Enabled
switch#
```

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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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 | ipv6-address]
```

Syntax Description

<i>hostname</i>	(Optional) RADIUS server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
<i>ipv4-address</i>	(Optional) RADIUS server IPv4 address in the <i>A.B.C.D</i> format.
<i>ipv6-address</i>	(Optional) RADIUS server IPv6 address in the <i>X:X::X:X</i> format.
directed-request	(Optional) Displays the directed request configuration.
groups [group-name]	(Optional) Displays information about the configured RADIUS server groups. Supply a <i>group-name</i> to display information about a specific 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
4.0(0)N1(1a)	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
retransmission count:1
timeout value:5
deadtime value:0
source interface:any available
total number of servers:1

following RADIUS servers are configured:
  192.168.1.1:
    available for authentication on port:1812
    available for accounting on port:1813
    RADIUS shared secret:*****

switch#
```

Send comments to nexus5k-docfeedback@cisco.com

This example shows how to display information for a specified RADIUS server:

```
switch# show radius-server 192.168.1.1
192.168.1.1:
    available for authentication on port:1812
    available for accounting on port:1813
    RADIUS shared secret:*****
    idle time:0
    test user:test
    test password:*****
switch#
```

This example shows how to display the RADIUS directed request configuration:

```
switch# show radius-server directed-request
disabled
switch#
```

This example shows how to display information for RADIUS server groups:

```
switch# show radius-server groups
total number of groups:2

following RADIUS server groups are configured:
group radius:
    server: all configured radius servers
    deadtime is 0
group RadServer:
    server: 192.168.1.1 on auth-port 1812, acct-port 1813
    deadtime is 0
switch#
```

This example shows how to display information for a specified RADIUS server group:

```
switch# show radius-server groups RadServer
group RadServer:
    server: 10.193.128.5 on auth-port 1812, acct-port 1813
    deadtime is 0
switch#
```

This example shows how to display sorted information for all RADIUS servers:

```
switch# show radius-server sorted
timeout value:5
retransmission count:1
deadtime value:0
source interface:any available
total number of servers:1

following RADIUS servers are configured:
192.168.1.1:
    available for authentication on port:1812
    available for accounting on port:1813
    RADIUS shared secret:*****
switch#
```

This example shows how to display statistics for a specified RADIUS servers:

```
switch# show radius-server statistics 192.168.1.1
Server is not monitored

Authentication Statistics
    failed transactions: 0
    sucessfull transactions: 0
```

Send comments to nexus5k-docfeedback@cisco.com

```

requests sent: 0
requests timed out: 0
responses with no matching requests: 0
responses not processed: 0
responses containing errors: 0

Accounting Statistics
  failed transactions: 0
  sucessfull transactions: 0
  requests sent: 0
  requests timed out: 0
  responses with no matching requests: 0
  responses not processed: 0
  responses containing errors: 0
switch#

```

Related Commands

Command	Description
show running-config radius	Displays the RADIUS information in the running configuration file.

Send comments to nexus5k-docfeedback@cisco.com

show role

To display the user role configuration, use the **show role** command.

show role [*name role-name*]

Syntax Description	name <i>role-name</i> (Optional) Displays information for a specific user role name.				
Command Default	Displays information for all user roles.				
Command Modes	EXEC mode				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>4.0(0)N1(1a)</td><td>This command was introduced.</td></tr> </table>	Release	Modification	4.0(0)N1(1a)	This command was introduced.
Release	Modification				
4.0(0)N1(1a)	This command was introduced.				

Examples

This example shows how to display information for a specific user role:

```
switch# show role name MyRole
```

```
Role: MyRole
```

```
Description: new role
vsan policy: permit (default)
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

```
-----
Rule      Perm      Type      Scope      Entity
-----
1         deny      command
                                pwd
-----
```

```
switch#
```

This example shows how to display information for all user roles:

```
switch# show role
```

In Cisco NX-OS Release 5.0(2)N1(1), the following output is displayed:

```
switch# show role
```

```
Role: network-admin
```

```
Description: Predefined network admin role has access to all commands
on the switch
```

```
-----
Rule      Perm      Type      Scope      Entity
-----
1         permit   read-write
```

```
Role: network-operator
```

```
Description: Predefined network operator role has access to all read
commands on the switch
```

```
-----
```

Send comments to nexus5k-docfeedback@cisco.com

Rule	Perm	Type	Scope	Entity
1	permit	read		

Role: vdc-admin

Description: Predefined vdc admin role has access to all commands within a VDC instance

Rule	Perm	Type	Scope	Entity
1	permit	read-write		

Role: vdc-operator

Description: Predefined vdc operator role has access to all read commands within a VDC instance

Rule	Perm	Type	Scope	Entity
1	permit	read		

Role: priv-14

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Rule	Perm	Type	Scope	Entity
1	permit	read-write		

Role: priv-13

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Role: priv-12

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Role: priv-11

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Role: priv-10

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Role: priv-9

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Send comments to nexus5k-docfeedback@cisco.com

Vrf policy: permit (default)

Role: priv-8

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Role: priv-7

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Role: priv-6

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Role: priv-5

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Role: priv-4

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Role: priv-3

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Role: priv-2

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Role: priv-1

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Role: priv-0

Description: This is a system defined privilege role.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Send comments to nexus5k-docfeedback@cisco.com

Rule	Perm	Type	Scope	Entity
10	permit	command		traceroute6 *
9	permit	command		traceroute *
8	permit	command		telnet6 *
7	permit	command		telnet *
6	permit	command		ping6 *
5	permit	command		ping *
4	permit	command		ssh6 *
3	permit	command		ssh *
2	permit	command		enable *

Role: default-role

Description: This is a system defined role and applies to all users.
 vsan policy: permit (default)
 Vlan policy: permit (default)
 Interface policy: permit (default)
 Vrf policy: permit (default)

Rule	Perm	Type	Scope	Entity
5	permit	command		feature environment
4	permit	command		feature hardware
3	permit	command		feature module
2	permit	command		feature snmp
1	permit	command		feature system

Role: priv-15

Description: This is a system defined privilege role.
 vsan policy: permit (default)
 Vlan policy: permit (default)
 Interface policy: permit (default)
 Vrf policy: permit (default)

Rule	Perm	Type	Scope	Entity
1	permit	read-write		

Role: MyRole

Description: new role
 vsan policy: permit (default)
 Vlan policy: permit (default)
 Interface policy: permit (default)
 Vrf policy: permit (default)

Rule	Perm	Type	Scope	Entity
1	deny	command		pwd

switch#

Related Commands

Command	Description
role name	Configures user roles.

Send comments to nexus5k-docfeedback@cisco.com

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 <i>feature-name</i>	(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
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to display the user role features:

```
switch# show role feature
```

In Cisco NX-OS Release 5.0(2)N1(1), the following output is displayed:

```
aaa                (AAA service related commands)
arp                (ARP protocol related commands)
cdp                (Cisco Discovery Protocol related commands)
l3vm               (Layer 3 virtualization related commands)
ping               (Network reachability test commands)
snmp               (SNMP related commands)
radius             (Radius configuration and show commands)
syslog             (Syslog related commands)
tacacs             (TACACS configuration and show commands)
install            (Software install related commands)
license            (License related commands)
callhome           (Callhome configuration and show commands)
platform           (Platform configuration and show commands)
access-list        (IP access list related commands)
svi                (Interface VLAN related commands)
vlan               (Virtual LAN related commands)
eth-span           (Ethernet SPAN related commands)
ethanalyzer        (Ethernet Analyzer)
spanning-tree      (Spanning Tree protocol related commands)
acl                (FC ACL related commands)
sfm                (ISCSI flow related commands)
fcns               (Fibre Channel Name Server related commands)
fcsp               (Fibre Channel Security Protocol related commands)
fdmi               (FDMI related commands)
fspf               (Fabric Shortest Path First protocol related commands)
rlir               (Registered Link Incident Report related commands)
rscn               (Registered State Change Notification related commands)
```

Send comments to nexus5k-docfeedback@cisco.com

```
span          (SPAN session relate commands)
vsan          (VSAN configuration and show commands)
wwnm         (WorldWide Name related commands)
zone         (Zone related commands)
fcanalyzer   (FC analyzer related commands)
switch#
```

This example shows how to display detailed information all the user role features:

```
switch# show role feature detail
```

In Cisco NX-OS Release 5.0(2)N1(1), the following output is displayed:

```
aaa          (AAA service related commands)
  show aaa *
  config t ; aaa *
  aaa *
  clear aaa *
  debug aaa *
  show accounting *
  config t ; accounting *
  accounting *
  clear accounting *
  debug accounting *
arp          (ARP protocol related commands)
  show ip arp *
  config t; ip arp *
  clear ip arp *
  debug ip arp *
  debug-filter ip arp *
cdp         (Cisco Discovery Protocol related commands)
  show cdp *
  config t ; cdp *
  cdp *
  clear cdp *
  debug cdp *
l3vm        (Layer 3 virtualization related commands)
  show vrf *
  config t ; vrf *
  routing-context vrf *
ping        (Network reachability test commands)
  show ping *
  config t ; ping *
  ping *
  clear ping *
  debug ping *
  show ping6 *
  config t ; ping6 *
  ping6 *
  clear ping6 *
  debug ping6 *
  show traceroute *
  config t ; traceroute *
--More--
switch#
```

This example shows how to display detailed information for a specific user role feature named arp:

```
switch# show role feature name arp
```

In Cisco NX-OS Release 5.0(2)N1(1), this command displays the following output:

```
arp          (ARP protocol related commands)
  show ip arp *
  config t; ip arp *
```

Send comments to nexus5k-docfeedback@cisco.com

```
clear ip arp *
debug ip arp *
debug-filter ip arp *
switch#
```

Related Commands

Command	Description
role feature-group	Configures feature groups for user roles.
rule	Configures rules for user roles.

Send comments to nexus5k-docfeedback@cisco.com

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 <i>group-name</i>	(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
	4.0(0)N1(1a)	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.

Send comments to nexus5k-docfeedback@cisco.com

show rollback log

To display the log of configuration rollbacks on the switch, use the **show rollback log** command.

show rollback log {exec | verify}

Syntax Description	exec	Displays the rollback execution log.
	verify	Displays the rollback verify log.

Command Default	None
-----------------	------

Command Modes	EXEC mode
---------------	-----------

Command History	Release	Modification
	5.0(2)N1(1)	This command was introduced.

Usage Guidelines	<p>If the rollback log is empty, the following message appears:</p> <pre>ERROR: Log Not Available</pre>
------------------	---

Examples	<p>This example shows how to display the rollback execution log:</p>
----------	--

```
switch# show rollback log exec
-----
time: Mon, 06:16:02 06 Sep 2010
Status: success
-----
time: Mon, 07:58:36 06 Sep 2010
Status: success
-----
time: Mon, 09:48:58 06 Sep 2010
Status: success
switch#
```

This example shows how to display the rollback verification log:

```
switch# show rollback log verify
-----
time: Mon, 09:48:56 06 Sep 2010
Status: success
-----
time: Mon, 09:48:58 06 Sep 2010
Status: success
switch#
```

Send comments to nexus5k-docfeedback@cisco.com

Related Commands	Command	Description
	rollback	Restores the active configuration to the checkpoint state.

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	This command was introduced.

Examples	<p>This example shows how to display the configured AAA information in the running configuration:</p> <pre>switch# show running-config aaa</pre>
----------	--

Related Commands	Command	Description
	aaa accounting default	Configures AAA methods for accounting.
	aaa authentication login console	Configures AAA authentication methods for console login.
	aaa authentication login default	Configures the default AAA authentication methods.
	aaa authentication login error-enable	Configures the AAA authentication failure message to display on the console.
	aaa authorization commands default	Configures default AAA authorization methods.
	aaa authorization config-commands default	Configures the default AAA authorization methods for all configuration commands.
	aaa group server radius	Creates a RADIUS server group.
	aaa user default-role	Enables the default role assigned by the AAA server administrator for remote authentication.

Send comments to nexus5k-docfeedback@cisco.com

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	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>5.0(2)N1(1)</td><td>This command was introduced.</td></tr> </table>	Release	Modification	5.0(2)N1(1)	This command was introduced.
Release	Modification				
5.0(2)N1(1)	This command was introduced.				

Examples

This example shows how to display the ACL running configuration:

```
switch# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Tue Aug 31 05:01:56 2010

version 5.0(2)N1(1)
ip access-list BulkData
  10 deny ip any any
ip access-list CriticalData
  10 deny ip any any
ip access-list Scavenger
  10 deny ip any any
mac access-list acl-mac
  10 permit any any
ip access-list denyv4
  20 deny ip 10.10.10.0/24 10.20.10.0/24 fragments
  30 permit udp 10.10.10.0/24 10.20.10.0/24 lt 400
  40 permit icmp any any router-advertisement
  60 deny tcp 10.10.10.0/24 10.20.10.0/24 syn
  70 permit igmp any any host-report
  80 deny tcp any any rst
  90 deny tcp any any ack
  100 permit tcp any any fin
  110 permit tcp any gt 300 any lt 400
  130 deny tcp any range 200 300 any lt 600
  140 deny tcp any range 200 300 any lt 600
ip access-list dot
  statistics per-entry
  10 permit ip 20.1.1.1 255.255.255.0 20.10.1.1 255.255.255.0 precedence flash-o
  verride
  :
<snip>
```

Send comments to nexus5k-docfeedback@cisco.com

```

:
vlan access-map vacl-mac
  match mac address acl-mac
  action forward
  statistics per-entry
vlan filter vacl-mac vlan-list 300

interface Ethernet1/1
  ipv6 port traffic-filter denv6 in

interface Ethernet1/2
  ip port access-group voice in

interface Ethernet1/9
  ipv6 port traffic-filter denv6 in

interface Ethernet1/10
  ipv6 port traffic-filter denv6 in

line vty
  access-class myACLlist in
  access-class myACLlist out
  ipv6 access-class myI6List out

switch#

```

This example shows how to display only the VTY running configuration:

```

switch# show running-config aclmgr | begin vty
line vty
  access-class myACLlist in
  access-class myACLlist out
  ipv6 access-class myI6List out

switch#

```

Related Commands

Command	Description
access-class	Configures access classes for VTY.
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.

Send comments to nexus5k-docfeedback@cisco.com

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(2)N1(1)	This command was introduced.

Examples This example shows how to display the ARP configuration:

```
switch# show running-config arp

!Command: show running-config arp
!Time: Mon Aug 23 07:33:15 2010

version 5.0(2)N1(1)
ip arp timeout 2100
ip arp event-history errors size medium

interface Vlan10
  ip arp 10.193.131.37 00C0.4F00.0000

switch#
```

This example shows how to display the ARP configuration with the default information:

```
switch# show running-config arp all

!Command: show running-config arp all
!Time: Mon Aug 23 07:33:52 2010

version 5.0(2)N1(1)
ip arp timeout 1500
ip arp event-history cli size small
ip arp event-history snmp size small
ip arp event-history client-errors size small
ip arp event-history client-event size small
ip arp event-history lcache-errors size small
ip arp event-history lcache size small
ip arp event-history errors size small
ip arp event-history ha size small
ip arp event-history event size small
ip arp event-history packet size small
```

Send comments to nexus5k-docfeedback@cisco.com

```
interface Vlan10
  ip arp 10.193.131.37 00C0.4F00.0000
  ip arp gratuitous update
  ip arp gratuitous request
```

```
switch#
```

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.

Send comments to nexus5k-docfeedback@cisco.com

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(2)N2(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

!Command: show running-config dhcp
!Time: Mon Aug 23 09:09:11 2010

version 5.0(2)N1(1)
feature dhcp

ip dhcp snooping
ip dhcp snooping information option
service dhcp
ip dhcp relay
ip dhcp relay information option

ip arp inspection filter arp-acl-01 vlan 15,37-48

switch#
```

This example shows how to display the DHCP snooping configuration with the default information:

```
switch# show running-config dhcp all

!Command: show running-config dhcp all
!Time: Mon Aug 23 09:10:11 2010

version 5.0(2)N1(1)
feature dhcp

ip dhcp snooping
```

Send comments to nexus5k-docfeedback@cisco.com

```
ip dhcp snooping information option
ip dhcp snooping verify mac-address
service dhcp
ip dhcp relay
ip dhcp relay information option
no ip dhcp relay sub-option type cisco
no ip dhcp relay information option vpn
no ip arp inspection validate src-mac dst-mac ip
ip arp inspection log-buffer entries 32
no ip dhcp packet strict-validation
```

```
interface port-channel23
  no ip dhcp snooping trust
  no ip arp inspection trust
  no ip verify source dhcp-snooping-vlan
```

```
interface port-channel67
  no ip dhcp snooping trust
  no ip arp inspection trust
  no ip verify source dhcp-snooping-vlan
```

```
interface port-channel150
  no ip dhcp snooping trust
  no ip arp inspection trust
  no ip verify source dhcp-snooping-vlan
```

```
interface port-channel400
  no ip dhcp snooping trust
  no ip arp inspection trust
  no ip verify source dhcp-snooping-vlan
```

```
<--output truncated-->
switch#
```

This example shows how to display the DHCP snooping configuration and the IP Source Guard information on a switch that runs Cisco NX-OS Release 5.0(3)N1(1):

```
switch# show running-config dhcp
```

```
!Command: show running-config dhcp
!Time: Sat Apr 19 06:18:33 2008
```

```
version 5.0(3)N1(1)
feature dhcp
```

```
ip dhcp snooping
ip dhcp snooping information option
```

```
interface Ethernet1/2
  ip dhcp snooping trust
  ip verify source dhcp-snooping-vlan
```

```
interface Ethernet1/5
  ip verify source dhcp-snooping-vlan
ip source binding 10.0.0.7 002f.23bd.0014 vlan 5 interface Ethernet1/2
ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface Ethernet1/5
```

```
switch#
```

Send comments to nexus5k-docfeedback@cisco.com

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.
	ip verify source	Enables IP Source Guard on a Layer 2 interface.
	show ip dhcp snooping	Displays general information about DHCP snooping.
	show ip verify source	Displays the IP-MAC address bindings.
	show startup-config dhcp	Displays the DHCP startup configuration.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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
	4.0(0)N1(1a)	This command was introduced.

Examples This example shows how to display information for RADIUS in the running configuration:

```
switch# show running-config radius
```

In Cisco NX-OS Release 5.0(2)N1(1), the following output is displayed:

```
!Command: show running-config radius
!Time: Wed Aug 25 10:25:41 2010

version 5.0(2)N1(1)
radius-server host 192.168.1.1 key 7 "KkwyCet" authentication accounting
aaa group server radius r1
    server 192.168.1.1

switch#
```

Related Commands	Command	Description
	show radius-server	Displays RADIUS information.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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
	4.0(0)N1(1a)	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
```

In Cisco NX-OS Release 5.0(2)N1(1), the following output is displayed:

```
!Command: show running-config security
!Time: Wed Aug 25 10:27:20 2010

version 5.0(2)N1(1)
feature telnet

username admin password 5 $1$eKzwPRms$5QB0PxpKXdp6ZKkME/vSS1 role network-admin
username praveena password 5 $1$9w6ZnM/R$Pg5OfsV/vkOaAGW.f.RyP. role network-operator
username install password 5 ! role network-admin
username user1 password 5 ! role priv-5
no password strength-check

switch#
```

Related Commands	Command	Description
	ssh	Creates a Secure Shell (SSH) connection using IPv4.
	ssh6	Creates a Secure Shell (SSH) connection using IPv6.
	telnet	Creates a Telnet session using IPv4.

Send comments to nexus5k-docfeedback@cisco.com

Command	Description
telnet6	Creates a Telnet session using IPv6.
username	Configures a user account.

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	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
```

In Cisco NX-OS Release 5.0(2)N1(1), the following output is displayed:

```
*****
rsa Keys generated:Mon Aug  2 22:49:27 2010

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA0iACA1fHAeIaY6PD5fSBLqGX3MIn+k72qhdvLNib7dL7
8CRQVS1AlQiDDTrvyIfRZ5yHMDQndvcmRfkJzluSCW2FP8vokZ66aXFk8TBTFc5Bn3NUiUyPZyhPtFD2
LaHBCkx10MxEP+nmPJ6Qf6mBzZVAIdLw8Nd64ZwqVHHjeFc=

bitcount:1024
fingerprint:
bb:bf:a4:c0:22:3b:70:15:e4:2b:2b:bb:08:41:82:d4
*****
could not retrieve dsa key information
*****
switch#
```

Related Commands	Command	Description
	ssh server key	Configures the SSH server key.

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	This command was introduced.

Examples	This example shows how to display the SSH server status:
-----------------	--

```
switch# show ssh server  
ssh version 2 is enabled  
switch#
```

Related Commands	Command	Description
	ssh server enable	Enables the SSH server.

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	This command was introduced.

Examples	<p>This example shows how to display the AAA information in the startup configuration:</p> <pre>switch# show startup-config aaa</pre>
-----------------	---

Related Commands	Command	Description
	show running-config aaa	Displays AAA configuration information in the running configuration.

Send comments to nexus5k-docfeedback@cisco.com

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(2)N1(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 31 05:01:58 2010

version 5.0(2)N1(1)
ip access-list BulkData
  10 deny ip any any
ip access-list CriticalData
  10 deny ip any any
ip access-list Scavenger
  10 deny ip any any
mac access-list acl-mac
  10 permit any any
ip access-list denyv4
  20 deny ip 10.10.10.0/24 10.20.10.0/24 fragments
  30 permit udp 10.10.10.0/24 10.20.10.0/24 lt 400
  40 permit icmp any any router-advertisement
  60 deny tcp 10.10.10.0/24 10.20.10.0/24 syn
  70 permit igmp any any host-report
  80 deny tcp any any rst
  90 deny tcp any any ack
  100 permit tcp any any fin
  110 permit tcp any gt 300 any lt 400
  130 deny tcp any range 200 300 any lt 600
  140 deny tcp any range 200 300 any lt 600
:
<snip>
:
vlan access-map vacl-mac
  match mac address acl-mac
  action forward
```

Send comments to nexus5k-docfeedback@cisco.com

```

statistics per-entry
vlan filter vacl-mac vlan-list 300

interface Ethernet1/1
  ipv6 port traffic-filter deny6 in

interface Ethernet1/2
  ip port access-group voice in

interface Ethernet1/9
  ipv6 port traffic-filter deny6 in

interface Ethernet1/10
  ipv6 port traffic-filter deny6 in

line vty
  access-class myACLlist in
  access-class myACLlist out
  ipv6 access-class myI6List out

switch#

```

This example shows how to display only the VTY startup configuration:

```

switch# show startup-config aclmgr | begin vty
line vty
  access-class myACLlist in
  access-class myACLlist out
  ipv6 access-class myI6List out

switch#

```

Related Commands

Command	Description
access-class	Configures access classes for VTY.
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 running-config aclmgr	Displays the ACL running configuration.

Send comments to nexus5k-docfeedback@cisco.com

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(2)N1(1)	This command was introduced.

Examples	<p>This example shows how to display the ARP startup configuration:</p> <pre>switch# show startup-config arp !Command: show running-config arp !Time: Mon Aug 23 07:33:15 2010 version 5.0(2)N1(1) ip arp timeout 2100 ip arp event-history errors size medium interface Vlan10 ip arp 10.193.131.37 00C0.4F00.0000 switch#</pre>
----------	---

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.

Send comments to nexus5k-docfeedback@cisco.com

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(2)N2(1)	This command was introduced.
Usage Guidelines	To use this command, you must enable the DHCP snooping feature using the feature dhcp command.	
Examples	<p>This example shows how to display the DHCP snooping configuration in the startup configuration file:</p> <pre>switch# show startup-config dhcp !Command: show startup-config dhcp !Time: Mon Aug 23 09:09:14 2010 version 5.0(2)N1(1) feature dhcp ip dhcp snooping ip dhcp snooping information option service dhcp ip dhcp relay ip dhcp relay information option ip arp inspection filter arp-acl-01 vlan 15,37-48 switch#</pre>	
Related Commands	Command	Description
	copy running-config startup-config	Copies the running configuration to the startup configuration.

Send comments to nexus5k-docfeedback@cisco.com

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

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	This command was introduced.

Examples	<p>This example shows how to display the RADIUS information in the startup configuration:</p> <pre>switch# show startup-config radius</pre>
-----------------	---

Related Commands	Command	Description
	show running-config radius	Displays RADIUS server information in the running configuration.

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	This command was introduced.

Examples	<p>This example shows how to display the user account, SSH server, and Telnet server information in the startup configuration:</p> <pre>switch# show startup-config security</pre>
-----------------	---

Related Commands	Command	Description
	show running-config security	Displays user account, Secure Shell (SSH) server, and Telnet server information in the running configuration.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	
<i>hostname</i>	(Optional) TACACS+ server Domain Name Server (DNS) name. The maximum character size is 256.
<i>ip4-address</i>	(Optional) TACACS+ server IPv4 address in the <i>A.B.C.D</i> format.
<i>ip6-address</i>	(Optional) TACACS+ server IPv6 address in the <i>X:X:X::X</i> 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
	4.0(0)N1(1a)	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
```

Send comments to nexus5k-docfeedback@cisco.com

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.

Send comments to nexus5k-docfeedback@cisco.com

show telnet server

To display the Telnet server status, use the **show telnet server** command.

show telnet server

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	EXEC mode
----------------------	-----------

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.

Examples	<p>This example shows how to display the Telnet server status:</p> <pre>switch# show telnet server</pre>
-----------------	---

Related Commands	Command	Description
	telnet server enable	Enables the Telnet server.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	<i>name</i> (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
	4.0(0)N1(1a)	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

user:admin
    this user account has no expiry date
    roles:network-admin
user:mable
    this user account has no expiry date
    roles:network-operator
user:install
    this user account has no expiry date
    roles:network-admin
no password set. Local login not allowed
Remote login through RADIUS/TACACS+ is possible
user:user1
    this user account has no expiry date
    roles:priv-5
no password set. Local login not allowed
Remote login through RADIUS/TACACS+ is possible
switch#
```

This example shows how to display information about a specific user account:

```
switch# show user-account admin
user:admin
    this user account has no expiry date
    roles:network-admin
switch#
```

Related Commands	Command	Description
	username	Configures a user account.

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	This command was introduced.

Examples	This example shows how to display all the users currently logged on the switch:
-----------------	---

```
switch# show users
NAME      LINE      TIME          IDLE          PID COMMENT
admin     ttyS0      Aug 24 22:19  10:41         4681
admin     pts/0      Aug 25 03:39   .             8890 (72.163.177.191) *
```

Related Commands	Command	Description
	clear user	Logs out a specific user.
	username	Creates and configures a user account.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	<i>map-name</i>	VLAN access list to show.
--------------------	-----------------	---------------------------

Command Default	None
-----------------	------

Command Modes	EXEC mode
---------------	-----------

Command History	Release	Modification
	4.0(0)N1(1a)	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	<p>This example shows how to display the contents of the ACL associated with the specified VLAN access map:</p> <pre>switch# show vlan access-list vlan1map</pre>
----------	---

Related Commands	Command	Description
	ip access-list	Creates or configures an IPv4 ACL.
	mac access-list	Creates or configures a MAC 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.
	show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.
	vlan access-map	Configures a VLAN access map.

Send comments to nexus5k-docfeedback@cisco.com

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	<i>map-name</i> (Optional) VLAN access map to show.	
Command Default	The switch shows all VLAN access maps, unless you use the <i>map-name</i> argument to select a specific access map.	
Command Modes	EXEC mode	
Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.
Usage Guidelines	<p>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.</p> <p>Use the show vlan filter command to see which VLANs have a VLAN access map applied to them.</p>	
Examples	<p>This example shows how to display a specific VLAN access map:</p> <pre>switch# show vlan access-map vlan1map</pre> <p>This example shows how to display all VLAN access maps:</p> <pre>switch# show vlan access-map Vlan access-map vacl-mac match mac: acl-mac action: forward statistics per-entry switch#</pre>	
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.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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 <i>map-name</i>	(Optional) Limits the output to VLANs that the specified access map is applied to.
vlan <i>vlan-id</i>	(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
4.0(0)N1(1a)	This command was introduced.

Examples

This example shows how to display all VLAN access map information on the switch:

```
switch# show vlan filter

vlan map vacl-mac:
    Configured on VLANs:    300
switch#
```

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.

Send comments to nexus5k-docfeedback@cisco.com



T Commands

This chapter describes the Cisco NX-OS security commands that begin with T.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

tacacs-server deadline

To set a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **tacacs-server deadline** command. To disable the monitoring of the nonresponsive TACACS+ server, use the **no** form of this command.

tacacs-server deadline *minutes*

no tacacs-server deadline *minutes*

Syntax Description	<i>time</i> Time interval in minutes. The range is from 1 to 1440.									
Command Default	0 minutes									
Command Modes	Global configuration mode									
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(0)N1(1a)</td><td>This command was introduced.</td></tr></table>		Release	Modification	4.0(0)N1(1a)	This command was introduced.				
Release	Modification									
4.0(0)N1(1a)	This command was introduced.									
Usage Guidelines	<p>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.</p> <p>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.</p> <p>You must use the feature tacacs+ command before you configure TACACS+.</p>									
Examples	<p>This example shows how to configure the dead-time interval and enable periodic monitoring:</p> <pre>switch(config)# tacacs-server deadtime 10</pre> <p>This example shows how to revert to the default dead-time interval and disable periodic monitoring:</p> <pre>switch(config)# no tacacs-server deadtime 10</pre>									
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>deadtime</td><td>Sets a dead-time interval for monitoring a nonresponsive RADIUS or TACACS+ server group.</td></tr><tr><td>feature tacacs+</td><td>Enables TACACS+.</td></tr><tr><td>show tacacs-server</td><td>Displays TACACS+ server information.</td></tr></table>		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.
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.									

Send comments to nexus5k-docfeedback@cisco.com

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
4.0(0)N1(1a)	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(config)# tacacs-server directed-request
```

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

```
switch(config)# no tacacs-server directed-request
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs-server directed request	Displays a directed request TACACS+ server configuration.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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

<i>hostname</i>	TACACS+ server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
<i>ipv4-address</i>	TACACS+ server IPv4 address in the <i>A.B.C.D</i> format.
<i>ipv6-address</i>	TACACS+ server IPv6 address in the <i>X:X:X::X</i> 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.
<i>shared-secret</i>	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 <i>port-number</i>	(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 <i>time</i>	(Optional) Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password <i>password</i>	(Optional) Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.
username <i>name</i>	(Optional) Specifies a user name in the test packets. The username is alphanumeric, case sensitive, and has a maximum of 32 characters.
timeout <i>seconds</i>	(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.

Send comments to nexus5k-docfeedback@cisco.com

Command Modes Global configuration mode

Command History	Release	Modification
	4.0(0)N1(1a)	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(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
```

Related Commands	Command	Description
	feature tacacs+	Enables TACACS+.
	show tacacs-server	Displays TACACS+ server information.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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.
	<i>shared-secret</i>	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
	4.0(0)N1(1a)	This command was introduced.

Usage Guidelines	<p>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.</p>
------------------	--

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

Examples	This example shows how to display configure TACACS+ server shared keys:
----------	---

```
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

Related Commands	Command	Description
	feature tacacs+	Enables TACACS+.
	show tacacs-server	Displays TACACS+ server information.

Send comments to nexus5k-docfeedback@cisco.com

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	<i>seconds</i>	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
	4.0(0)N1(1a)	This command was introduced.

Usage Guidelines	You must use the feature tacacs+ command before you configure TACACS+.
------------------	---

Examples	<p>This example shows how to configure the TACACS+ server timeout value:</p> <pre>switch(config)# tacacs-server timeout 3</pre> <p>This example shows how to revert to the default TACACS+ server timeout value:</p> <pre>switch(config)# no tacacs-server timeout 3</pre>
----------	--

Related Commands	Command	Description
	feature tacacs+	Enables TACACS+.
	show tacacs-server	Displays TACACS+ server information.

Send comments to nexus5k-docfeedback@cisco.com

telnet

To create a Telnet session using IPv4 on a Cisco Nexus 5000 Series switch, use the **telnet** command.

telnet {*ipv4-address* | *hostname*} [*port-number*] [**vrf** {*vrf-name* | **default** | **management**}]

Syntax Description	<i>ipv4-address</i>	IPv4 address of the remote switch.
	<i>hostname</i>	Hostname of the remote switch. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
	<i>port-number</i>	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
	vrf <i>vrf-name</i>	(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
	4.0(0)N1(1a)	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.

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	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.

Send comments to nexus5k-docfeedback@cisco.com

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		
	<i>ipv6-address</i>	IPv6 address of the remote device.
	<i>hostname</i>	Hostname of the remote device. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
	<i>port-number</i>	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
	vrf <i>vrf-name</i>	(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
	4.0(1a)N1(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.

Send comments to nexus5k-docfeedback@cisco.com



U Commands

This chapter describes the Cisco NX-OS security commands that begin with U.

Send comments to nexus5k-docfeedback@cisco.com

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

<i>vrf-name</i>	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

RADIUS server group configuration mode
TACACS+ server group configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure only one VRF instance for a server group.

Use the **aaa group server radius** command in 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(config)# aaa group server radius RadServer
switch(config-radius)# use-vrf management
```

This example shows how to specify a VRF instance for a TACACS+ server group:

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs)# use-vrf management
```

This example shows how to remove the VRF instance from a TACACS+ server group:

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs)# no use-vrf management
```

Send comments to nexus5k-docfeedback@cisco.com

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.

Send comments to nexus5k-docfeedback@cisco.com

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

<i>user-id</i>	User identifier for the user account. The <i>user-id</i> 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 <i>user-id</i> argument text string.
expire <i>date</i>	(Optional) Specifies the expire date for the user account. The format for the <i>date</i> 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.
<i>password</i>	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 <i>role-name</i>	(Optional) Specifies the role which the user is to be assigned to. Valid values are as follows: <ul style="list-style-type: none"> • 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

Send comments to nexus5k-docfeedback@cisco.com

	<ul style="list-style-type: none"> • 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 <i>level</i>	(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.
<i>key</i>	SSH key string.
filename <i>filename</i>	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
4.0(0)N1(1a)	This command was introduced.
5.0(2)N1(1)	The priv-lvl keyword was added.

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.

Send comments to nexus5k-docfeedback@cisco.com

Examples

This example shows how to create a user account with a password:

```
switch(config)# username user1 password Ci5co321
switch(config)#
```

This example shows how to configure the SSH key for a user account:

```
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(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.

Send comments to nexus5k-docfeedback@cisco.com



V Commands

This chapter describes the Cisco NX-OS security commands that begin with V.

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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	<i>map-name</i> 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													
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(0)N1(1a)</td><td>This command was introduced.</td></tr></table>		Release	Modification	4.0(0)N1(1a)	This command was introduced.								
Release	Modification													
4.0(0)N1(1a)	This command was introduced.													
Usage Guidelines	Each VLAN access map can include one match command and one action command.													
Examples	<p>This example shows how to create a VLAN access map named <code>vlan-map-01</code>, assign an IPv4 ACL named <code>ip-acl-01</code> to the map, specify that the switch forwards packets matching the ACL, and enable statistics for traffic matching the map:</p> <pre>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</pre>													
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>action</td><td>Specifies an action for traffic filtering in a VLAN access map.</td></tr><tr><td>match</td><td>Specifies an ACL for traffic filtering in a VLAN access map.</td></tr><tr><td>show vlan access-map</td><td>Displays all VLAN access maps or a VLAN access map.</td></tr><tr><td>show vlan filter</td><td>Displays information about how a VLAN access map is applied.</td></tr><tr><td>vlan filter</td><td>Applies a VLAN access map to one or more VLANs.</td></tr></table>		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.
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.													

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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

<i>map-name</i>	Name of the VLAN access map that you want to create or configure.
vlan-list <i>VLAN-list</i>	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 <i>VLAN-list</i> 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

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

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(config)# vlan filter vlan-map-01 20-45
```

Send comments to nexus5k-docfeedback@cisco.com

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 access-map	Configures a VLAN access map.

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	This command was introduced.

Examples	This example shows how to enter VLAN policy configuration mode for a user role:
-----------------	---

```
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
```

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

[Send comments to nexus5k-docfeedback@cisco.com](mailto:nexus5k-docfeedback@cisco.com)

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
4.0(0)N1(1a)	This command was introduced.

Examples

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

```
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(config)# role name MyRole
switch(config-role)# no vrf policy deny
```

Related Commands

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

Send comments to nexus5k-docfeedback@cisco.com

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
	4.0(0)N1(1a)	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(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(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.

Send comments to nexus5k-docfeedback@cisco.com