

Send comments to nexus5k-docfeedback@cisco.com



Preface

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

This preface includes the following sections:

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

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 ix](#)
- [Cisco Nexus 5500 Platform Switches, page x](#)

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](mailto: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](mailto: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 system management commands that begin with A.
C Commands	Describes the Cisco NX-OS system management commands that begin with C.
D Commands	Describes the Cisco NX-OS system management commands that begin with D.
I Commands	Describes the Cisco NX-OS system management commands that begin with I.
L Commands	Describes the Cisco NX-OS system management commands that begin with L.
N Commands	Describes the Cisco NX-OS system management commands that begin with N.
S Commands	Describes the Cisco NX-OS system management commands that begin with S.
Show Commands	Describes the Cisco NX-OS system management show commands.
V Commands	Describes the Cisco NX-OS system management commands that begin with V.
System Message Logging Facilities	Describes the Cisco NX-OS system message logging facilities.

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.
[]	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.

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

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

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

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

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)NI(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

Error and System Messages

Cisco NX-OS System Messages Reference

Send comments to nexus5k-docfeedback@cisco.com

Troubleshooting Guide

Cisco Nexus 5000 Troubleshooting Guide

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.

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 System Management 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\(5\)](#), page xv
- [New and Changed Information for Cisco NX-OS Release 5.2\(1\)N1\(1\)](#), page xvi
- [New and Changed Information for Cisco NX-OS Release 5.1\(3\)N1\(1\)](#), page xvi
- [New and Changed Information for Cisco NX-OS Release 5.0\(3\)N2\(1\)](#), page xvii
- [New and Changed Information for Cisco NX-OS Release 5.0\(3\)N1\(1\)](#), page xvii
- [New and Changed Information for Cisco NX-OS Release 5.0\(2\)N2\(1\)](#), page xviii
- [New and Changed Information for Cisco NX-OS Release 5.0\(2\)N1\(1\)](#), page xviii

New and Changed Information for Cisco NX-OS Release 5.2(1)N1(5)

[Table 1](#) summarizes the new and changed features for Cisco NX-OS Release 5.2(1)N1(5) and tells you where they are documented.

Table 1 *New and Changed Information for Release 5.2(1)N1(5)*

Feature	Description	Where Documented
DOM Enabling/Disabling and Monitoring	Adds the ability to enable and disable transceiver digital optical monitoring and display the status.	system ethernet dom polling show system ethernet dom polling status

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

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

Feature	Description	Where Documented
ACL logging	Added logging capability for ACLs on the mgmt0 interface.	acllog match-log-level logging ip access-list cache
PTP	Added the following commands: <ul style="list-style-type: none"> • feature ptp • ptp announce • ptp delay request minimum interval • ptp domain • ptp priority1 • ptp priority2 • ptp source • ptp sync interval • ptp vlan • show ptp brief • show ptp clock • show ptp clocks foreign-masters-record • show ptp corrections • show ptp parent • show ptp port interface • show ptp time-property 	F Commands P Commands Show Commands
Configuration Synchronization Enhancement	Configuration sychronization improvements for deleting and restoring switch profile configuration.	switch-profile

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

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

Send comments to nexus5k-docfeedback@cisco.com

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

Feature	Description	Where Documented
Domain Name Server (DNS) enhancements	The following commands were introduced: <ul style="list-style-type: none"> • ip dns source-interface • show ip dns source-interface 	
Simple Network Management Protocol (SNMP) enhancement	The following command was updated: <ul style="list-style-type: none"> • snmp trap link-status 	

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

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

Table 4 *New and Changed Information for Release 5.0(3)N1(1)*

Feature	Description	Where Documented
Domain Name System (DNS)	<p>This feature was introduced.</p> <p>The following DNS commands were introduced:</p> <ul style="list-style-type: none"> • ip domain-list • ip domain-lookup • ip domain-name • ip host • ip name-server • show hosts 	<p>ip domain-list</p> <p>ip domain-lookup</p> <p>ip domain-name</p> <p>ip host</p> <p>ip name-server</p> <p>show hosts</p>
Simple Network Management Protocol (SNMP)	<p>Added the following SNMP commands:</p> <p>Note These commands were missing from the previous releases of the document.</p> <ul style="list-style-type: none"> • snmp-server contact • snmp-server context • snmp-server enable traps • snmp-server enable traps link • snmp-server globalEnforcePriv • snmp-server host • snmp-server location • snmp-server mib community-map • snmp-server tcp-session • snmp-server user • snmp trap link-status • show snmp user 	<p>snmp-server contact</p> <p>snmp-server context</p> <p>snmp-server enable traps</p> <p>snmp-server enable traps link</p> <p>snmp-server globalEnforcePriv</p> <p>snmp-server host</p> <p>snmp-server location</p> <p>snmp-server mib community-map</p> <p>snmp-server tcp-session</p> <p>snmp-server user</p> <p>snmp trap link-status</p> <p>show snmp context</p> <p>show snmp engineID</p> <p>show snmp group</p> <p>show snmp host</p> <p>show snmp sessions</p> <p>show snmp trap</p> <p>show snmp user</p>

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

There are no new and changed features for Cisco NX-OS Release 5.0(2)N2(1).

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.

Send comments to nexus5k-docfeedback@cisco.com

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)			
SNMP notification for VTP domain	You can enable SNMP notifications for a VTP domain.	5.0(2)N1(1)	snmp-server globalEnforcePriv

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com



A Commands

This chapter describes the system management commands that begin with A.

Send comments to nexus5k-docfeedback@cisco.com

abort (session)

To discard the current configuration session, use the **abort** command.

abort

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Session configuration mode

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

Examples This example shows how to abort the current configuration session:

```
switch# configure session MySession1
switch(config-s)# abort
switch#
```

Related Commands	Command	Description
	commit	Commits a session.
	configure session	Creates a configuration session.
	show configuration session	Displays the contents of the session.
	verify	Verifies a session.

Send comments to nexus5k-docfeedback@cisco.com

acllog match-log-level

To specify the minimum severity level to log ACL matches, use the **acllog match-log-level** command. To remove the acllog match log level, use the **no** form of this command.

acllog match-log-level *severity-level*

no acllog match-log-level *severity-level*

Syntax Description	<i>severity-level</i>	<p>Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows:</p> <ul style="list-style-type: none"> • 0—emergency: System unusable • 1—alert: Immediate action needed • 2—critical: Critical condition • 3—error: Error condition • 4—warning: Warning condition • 5—notification: Normal but significant condition—default level • 6—informational: Informational message only (default) • 7—debugging: Appears during debugging only
---------------------------	-----------------------	---

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

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

Command History	Release	Modification
	5.2(1)N1(1)	This command was introduced.

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

```
switch(config)# acllog match-log-level 6
switch(config)#
```

Related Commands	Command	Description
	logging level	Enables logging messages from a specified facility and configures the logging severity level.
	logging logfile	Configures the name of the log file used to store system messages and sets the minimum severity level to log.

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com



C Commands

This chapter describes the system management commands that begin with C.

Send comments to nexus5k-docfeedback@cisco.com

clear logging logfile

To clear the contents of the log file, use the **clear logging logfile** command.

clear logging logfile

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

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

Examples This example shows how to clear the logging logfile:

```
switch# clear logging logfile
switch#
```

Related Commands	Command	Description
	show logging logfile	Displays the messages in the log file.

Send comments to nexus5k-docfeedback@cisco.com

clear logging nvram

To clear the NVRAM logs, use the **clear logging nvram** command.

```
clear logging nvram
```

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 clear the NVRAM logs:

```
switch# clear logging nvram
```

Related Commands	Command	Description
	show logging nvram	Displays the NVRAM logs.

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

clear logging onboard

To clear the onboard failure logging (OBFL) entries in the persistent log, use the **clear logging onboard** command.

clear logging onboard [**environmental-history**] [**exception-log**] [**obfl-log**] [**stack-trace**]

Syntax Description	
environmental-history	(Optional) Clears the OBFL environmental history.
exception-log	(Optional) Clears the OBFL exception log entries.
obfl-log	(Optional) Clears the OBFL (boot-uptime/device-version/obfl-history).
stack-trace	(Optional) Clears the OBFL stack trace entries.

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 the OBFL environmental history entries:

```
switch# clear logging onboard environmental-history
```

This example shows how to clear the OBFL exception-log entries:

```
switch# clear logging onboard exception-log
```

This example shows how to clear the OBFL (boot-uptime/device-version/obfl-history) entries:

```
switch# clear logging onboard obfl-log
```

This example shows how to clear the OBFL stack trace entries:

```
switch# clear logging onboard stack-trace
```

Related Commands	Command	Description
	show logging onboard	Displays onboard failure logs.

Send comments to nexus5k-docfeedback@cisco.com

clear logging session

To clear the current logging session, use the **clear logging session** command.

clear logging session

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 clear the current logging session:

```
switch# clear logging session
```

Related Commands	Command	Description
	show logging session	Displays the logging session status.

Send comments to nexus5k-docfeedback@cisco.com

clear ntp session

To clear the Network Time Protocol (NTP) session, use the **clear ntp session** command.

clear ntp session

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 discard the NTP Cisco Fabric Services (CFS) distribution session in progress:

```
switch# clear ntp session
```

Related Commands	Command	Description
	show ntp	Displays NTP information.

Send comments to nexus5k-docfeedback@cisco.com

clear ntp statistics

To clear the Network Time Protocol (NTP) session, use the **clear ntp statistics** command.

```
clear ntp statistics {all-peers | io | local | memory}
```

Syntax Description		
	all-peers	Clears all peer transaction statistics.
	io	Clears I/O statistics.
	local	Clears local statistics.
	memory	Clears memory statistics.

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 discard the NTP I/O statistics:

```
switch# clear ntp statistics io
```

Related Commands	Command	Description
	show ntp	Displays NTP information.

Send comments to nexus5k-docfeedback@cisco.com

commit (session)

To commit the current configuration session, use the **commit** command.

commit

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Session configuration mode

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

Examples This example shows how to commit the current session:

```
switch(config-s)# commit
switch(config-s)#
```

Related Commands	Command	Description
	configure session	Creates a configuration session.
	show configuration session	Displays the contents of the session.
	verify	Verifies a session.

Send comments to nexus5k-docfeedback@cisco.com



D Commands

This chapter describes the system management commands that begin with D.

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

diagnostic bootup level

To configure the bootup diagnostic level to trigger diagnostics when the device boots, use the **diagnostic bootup level** command. To remove bootup diagnostic level configuration, use the **no** form of this command.

diagnostic bootup level {bypass | complete}

no diagnostic bootup level {bypass | complete}

Syntax Description

bypass	Specifies that all bootup tests are skipped.
complete	Specifies that all bootup diagnostics are performed. This is the default value.

Command Default

Complete

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1)	This command was introduced.
4.2(1)N2(1)	Support was added to control the diagnostic level of all the Cisco Nexus 2000 Series Fabric Extenders connected to the switch.

Examples

This example shows how to configure the bootup diagnostics level to trigger the complete diagnostics:

```
switch(config)# diagnostic bootup level complete
switch(config)#
```

This example shows how to remove the bootup diagnostics level configuration:

```
switch(config)# no diagnostic bootup level complete
switch(config)#
```

Related Commands

Command	Description
show diagnostic bootup level	Displays the bootup diagnostics level.
show diagnostic bootup result	Displays the results of the diagnostics tests.

Send comments to nexus5k-docfeedback@cisco.com



F Commands

This chapter describes the system management commands that begin with F.

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

feature ptp

To enable the PTP feature, use the **feature ptp** command. To unconfigure the PTP feature, use the **no** form of this command.

feature ptp

no feature ptp

Syntax Description There are no arguments or keywords for this command.

Command Default None

Command Modes Global configuration mode

Command History	Release	Modification
	5.2(1)N1(1)	This command was introduced.

Examples This example shows how to enable PTP on the device:

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

Related Commands	Command	Description
	feature ptp	Enables or disables PTP on the device.
	ptp source	Configures the source IP address for all PTP packets.
	ptp domain	Configures the domain number to use for this clock.
	ptp priority1	Configures the priority 1 value to use when advertising this clock.
	ptp priority2	Configures the priority 1 value to use when advertising this clock.
	show ptp brief	Displays the PTP status.
	show ptp clock	Displays the properties of the local clock.

Send comments to nexus5k-docfeedback@cisco.com



I Commands

This chapter describes the system management commands that begin with I.

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

ip access-list (session)

To create an IPv4 access control list (ACL) within a configuration session, use the **ip access-list** command. To remove an ACL from a configuration session, use the **no** form of this command.

ip access-list *ACL-name*

no ip access-list *ACL-name*

Syntax Description	<i>ACL-name</i>	Name of the IPv4 ACL. The name can be up to 64 alphanumeric characters and cannot contain a space or quotation mark.
Command Default	No IPv4 ACLs are defined by default.	
Command Modes	Global session configuration mode	
Command History	Release	Modification
	4.0(0)N1(1)	This command was introduced.
Examples	This example shows how to create an IPv4 ACL for a configuration session:	
	<pre>switch# configure session MySession1 switch(config-s)# ip access-list myACL switch(config-s-acl)#</pre>	
Related Commands	Command	Description
	configure session	Creates a configuration session.
	deny	Configures a deny rule in an IPv4 ACL.
	permit	Configures a permit rule in an IPv4 ACL.
	show configuration session	Displays the contents of the session.

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

ip dns source-interface

To configure the source interface for the Domain Name Server (DNS) domain lookup, use the **ip dns source-interface** command. To revert to the default settings, use the **no** form of this command.

```
ip dns source-interface { ethernet slot/port | loopback intf-num } [vrf { vrf-name | default | management }]
```

```
no ip dns source-interface { ethernet slot/port | loopback intf-num } [vrf { vrf-name | default | management }]
```

Syntax Description

ethernet <i>slot/port</i>	Specifies the Ethernet interface to use as the source interface. The slot number is from 1 to 255 and the port number is from 1 to 128.
loopback <i>intf-num</i>	Specifies the loopback interface to use as the source interface. The range of values is from 0 to 1023.
vrf	(Optional) Specifies the virtual routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) VRF name. The name is case sensitive and can be a maximum of 32 characters.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

None

Command Modes

Global configuration 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 configure an Ethernet interface as the source interface for a DNS lookup:

```
switch# configure terminal
switch(config)# ip dns source-interface ethernet 1/5
switch(config)#
```

Related Commands

Command	Description
ip domain-lookup	Enables the DNS lookup feature.
show ip dns source-interface	Displays information about the DNS source interfaces.

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

ip domain-list

To configure the IP domain list, use the **ip domain-list** command. To disable the IP domain list, use the **no** form of the command.

ip domain-list *domain-name* [**use-vrf** *name*]

no ip domain-list *domain-name* [**use-vrf** *name*]

Syntax Description	domain-list	Specifies the domain name for the IP domain list. The name can be any case-sensitive, alphanumeric string up to 63 characters.
	use-vrf <i>name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) to use to resolve the domain domain name for the IP domain list. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default None

Command Modes Global configuration mode
VRF context configuration mode

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

Usage Guidelines Use the **ip domain-list** command to configure additional domain names for the device. Use the **vrf context** command to enter the VRF context mode to configure additional domain names for a particular VRF.

Examples This example shows how to configure the IP domain list for the default VRF:

```
switch# config terminal
switch(config)# ip domain-list Mysite.com
```

This example shows how to configure the IP domain list for the management VRF:

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# ip domain-list Mysite.com
```

This example shows how to configure the IP domain list for the default VRF to use the management VRF as a backup if the domain name cannot be resolved through the default VRF:

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# exit
switch(config)# ip domain-name Mysite.com use-vrf management
switch(config)# ip name-server 192.0.2.1
switch(config)# ip domain-list Mysite2.com
```


Send comments to nexus5k-docfeedback@cisco.com

Related Commands	Command	Description
	show hosts	Displays information about the IP domain name configuration.

Send comments to nexus5k-docfeedback@cisco.com

ip domain-lookup

To enable the Domain Name Server (DNS) lookup feature, use the **ip domain-lookup** command. Use the **no** form of this command to disable this feature.

ip domain-lookup

no ip domain-lookup

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration mode

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

Usage Guidelines Use the **ip domain-lookup** command to enable DNS.

Examples This example shows how to configure the DNS server lookup feature:

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# exit
switch(config)# ip domain-name Mysite.com use-vrf management
switch(config)# ip name-server 192.0.2.1
switch(config)# ip domain-lookup
switch(config)#
```

Related Commands	Command	Description
	show hosts	Displays information about the DNS.

Send comments to nexus5k-docfeedback@cisco.com

ip domain-name

To configure a domain name, use the **ip domain-name** command. To delete a domain name, use the **no** form of the command.

ip domain-name *domain-name* [**use-vrf** *name*]

no ip domain-name *domain-name* [**use-vrf** *name*]

Syntax Description	
<i>domain-name</i>	Domain name. The name can be any case-sensitive, alphanumeric string up to 63 characters.
use-vrf <i>name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) to use to resolve the domain name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default None

Command Modes Global configuration mode
VRF context configuration mode

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

Usage Guidelines Use the **ip domain-name** command to configure the domain name for the device. Use the **vrf context** command to enter the VRF context mode to configure the domain monastery for a particular VRF.

Examples This example shows how to configure the IP domain name for the default VRF:

```
switch# config terminal
switch(config)# ip domain-name Mysite.com
switch(config)#
```

This example shows how to configure the IP domain name for the management VRF:

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# ip domain-name Mysite.com
switch(config-vrf)#
```

This example shows how to configure the IP domain name for the default VRF to use the management VRF as a backup if the domain name cannot be resolved through the default VRF:

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# exit
switch(config)# ip domain-name Mysite.com use-vrf management
```

Send comments to nexus5k-docfeedback@cisco.com

Related Commands

Command	Description
ip domain-list	Configures the IP domain list.
ip domain-lookup	Enables the Domain Name Server (DNS) lookup feature.
show hosts	Displays information about the IP domain name configuration.

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

ip host

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache, use the **ip host** command. To remove a hostname-to-address mapping, use the **no** form of this command.

ip host *name* *address1* [*address2...* *address6*]

no ip host *name* *address1* [*address2...* *address6*]

Syntax Description	
<i>name</i>	Hostname. The <i>name</i> can be any case-sensitive, alphanumeric string up to 80 characters.
<i>address1</i>	IPv4 address in the x.x.x.x format.
<i>address2 ...address6</i>	(Optional) Up to five additional IPv4 addresses in the x.x.x.x format.

Command Default None

Command Modes Global configuration mode

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

Usage Guidelines Use the **ip host** command to add a static hostname to DNS.

Examples This example shows how to configure a static hostname:

```
switch(config)# ip host mycompany.com 192.0.2.1
```

Related Commands	Command	Description
	show hosts	Displays information about the IP domain name configuration.

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

ip name-server

To configure a name server, use the **ip name-server** command. To disable this feature, use the **no** form of the command.

```
ip name-server ip-address [use-vrf name]
```

```
no ip name-server ip-address [use-vrf name]
```

Syntax Description		
	<i>ip-address</i>	IP address for the name server.
	use-vrf <i>name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) to use to reach the name-server. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default	
	None

Command Modes	
	Global configuration mode VRF context configuration mode

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

Usage Guidelines	
	Use the ip name-server command to configure the name server for the device. Use the vrf context command to enter the VRF context mode to configure the domain names for a particular VRF.

Examples	
	This example shows how to configure the IP name server for the default VRF:

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# exit
switch(config)# ip domain-name Mysite.com use-vrf management
switch(config)# ip name-server 192.0.2.1
```

This example shows how to configure the IP name server for the management VRF:

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# ip name-server 192.0.2.1
```

This example shows how to configure the IP name server for the default VRF to use the management VRF as a backup if the IP name server cannot be reached through the default VRF:

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# exit
switch(config)# ip domain-name Mysite.com use-vrf management
switch(config)# ip name-server 192.0.2.1 use-vrf management
```

Send comments to nexus5k-docfeedback@cisco.com

Related Commands	Command	Description
	ip domain-list	Defines a list of domains.
	ip domain lookup	Enables DNS-based host name-to-address translation.
	show hosts	Displays information about the IP domain name configuration.
	vrf context	Creates a virtual routing and forwarding (VRF) instance.

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

ip port access-group (session)

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** | **out**}

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

Syntax Description

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

Command Default

None

Command Modes

Session interface configuration mode

Command History

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

Examples

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

```
switch# configure session MySession1
switch(config-s)# interface ethernet 1/2
switch(config-s-if)# ip port access-group ip-acl-01 in
switch(config-s-if)#
```

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

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

Related Commands

Command	Description
show access-lists	Displays all ACLs.
show configuration session	Displays the contents of the session.

Send comments to nexus5k-docfeedback@cisco.com



L Commands

This chapter describes the system management commands that begin with L.

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

locator-led

To turn on the locator LED of a Fabric Extender, use the **locator-led** command. To turn off the locator LED, use the **no** form of this command.

```
locator-led {chassis pattern {long| medium | short} | fex fex_number}
```

```
no locator-led {chassis pattern {long| medium | short} | fex fex_number}
```

Syntax Description

chassis	Specifies the Blink chassis LED.
pattern	Specifies the LED blink pattern.
long	Specifies a long LED blink.
medium	Specifies a medium LED blink.
short	Specifies a short LED blink.
<i>fex_number</i>	Fabric Extender number. The range is from 100 to 199.

Command Default

None

Command Modes

EXEC mode

Command History

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

Usage Guidelines

Use the **locator-led** command to toggle the locator LED of a Fabric Extender, which allows you to easily identify the machine in a busy data center.

Examples

This example shows how to turn on the locator LED for a specific Fabric Extender chassis:

```
switch# locator-led fex 100
switch#
```

This example shows how to turn off the locator beacon LED for a specific Fabric Extender chassis:

```
switch# no locator-led fex 100
switch#
```

Related Commands

Command	Description
show fex	Displays all configured Fabric Extender chassis connected to the switch.
show locator-led	Displays the status of the locator LED in Fabric Extender modules.

Send comments to nexus5k-docfeedback@cisco.com

logging abort

To discard the pending changes to the syslog server configuration, use the **logging abort** command.

logging abort

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration mode

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

Examples This example shows how to discard the changes made to the syslog server configuration:

```
switch(config)# logging distribute
switch(config)# logging abort
switch(config)#
```

Related Commands	Command	Description
	logging distribute	Enables the distribution of the syslog server configuration to network switches using the CFS infrastructure.
	show logging pending	Displays the pending changes to the syslog server configuration.
	show logging status	Displays the logging status.

Send comments to nexus5k-docfeedback@cisco.com

logging commit

To commit the pending changes to the syslog server configuration for distribution to the switches in the fabric, use the **logging commit** command.

logging commit

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration mode

Command History

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

Examples

This example shows how to commit the distribution of the syslog server configuration:

```
switch(config)# logging distribute
switch(config)# commit
switch(config)#
```

Related Commands

Command	Description
logging distribute	Enables the distribution of the syslog server configuration to network switches using the CFS infrastructure.
show logging status	Displays the logging status.

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

logging console

To enable logging messages to the console session, use the **logging console** command. To disable logging messages to the console session, use the **no logging console** command.

logging console [*severity-level*]

no logging console

Syntax Description	<p><i>severity-level</i></p> <p>(Optional) Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows:</p> <ul style="list-style-type: none"> • 0—emergency: System unusable • 1—alert: Immediate action needed • 2—critical: Critical condition—default level • 3—error: Error condition • 4—warning: Warning condition • 5—notification: Normal but significant condition • 6—informational: Informational message only • 7—debugging: Appears during debugging only
---------------------------	---

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

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

Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(0)N1(1a)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(0)N1(1a)	This command was introduced.
Release	Modification				
4.0(0)N1(1a)	This command was introduced.				

Examples	<p>This example shows how to enable logging messages with a severity level of 4 (warning) or higher to the console session:</p> <pre>switch# configure terminal switch(config)# logging console 4</pre>
-----------------	---

Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>show logging console</td> <td>Displays the console logging configuration.</td> </tr> </tbody> </table>	Command	Description	show logging console	Displays the console logging configuration.
Command	Description				
show logging console	Displays the console logging configuration.				

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

logging distribute

To enable the distribution of the syslog server configuration to network switches using the Cisco Fabric Services (CFS) infrastructure, use the **logging distribute** command. To disable the distribution, use the **no** form of this command.

logging distribute

no logging distribute

Syntax Description This command has no arguments or keywords.

Command Default Distribution is disabled.

Command Modes Global configuration mode

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

Examples This example shows how to enable the distribution of the syslog server configuration:

```
switch(config)# logging distribute
switch(config)#
```

This example shows how to disable the distribution of the syslog server configuration:

```
switch(config)# no logging distribute
switch(config)#
```

Related Commands	Command	Description
	logging abort	Cancels the pending changes to the syslog server configuration.
	logging commit	Commits the changes to the syslog server configuration for distribution to the switches in the fabric.
	show logging status	Displays the logging status.

Send comments to nexus5k-docfeedback@cisco.com

logging event

To log interface events, use the **logging event** command. To disable logging of interface events, use the **no** form of this command.

logging event port {link-status | trunk-status} {default | enable}

no logging event port {link-status | trunk-status} {default | enable}

Syntax	Description
link-status	Specifies to log all UP/DOWN and CHANGE messages.
trunk-status	Specifies to log all TRUNK status messages.
default	Specifies to the default logging configuration is used by interfaces not explicitly configured.
enable	Enables the logging to override the port level configuration.

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 log interface events:

```
switch# configure terminal
switch(config)# logging event link-status default
```

Related Commands	Command	Description
	show logging	Displays the logging status.

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

logging event port

To log events on an interface, use the **logging event port** command. To disable logging of interface events, use the **no** form of this command.

logging event port {link-status | trunk-status} [default]

no logging event port {link-status | trunk-status}

Syntax Description	link-status	Specifies to log all UP/DOWN and CHANGE messages.
	trunk-status	Specifies to log all TRUNK status messages.
	default	(Optional) Specifies the default logging configuration that is used by interfaces not explicitly configured.

Command Default None

Command Modes Interface configuration mode

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

Examples This example shows how to log interface events:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# logging event port link-status default
```

Related Commands	Command	Description
	show interface	Displays the interface configuration information.
	show logging	Displays the logging status.

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

logging ip access-list cache

To configure the Optimized ACL Logging (OAL) parameters, use the **logging ip access-list cache** command. To reset to the default settings, use the **no** form of this command.

```
logging ip access-list cache {{entries num_entries} | {interval seconds} | {threshold
num_packets}}
```

```
no logging ip access-list cache {{entries num_entries} | {interval seconds} | {threshold
num_packets}}
```

Syntax Description

entries <i>num_entries</i>	Specifies the maximum number of log entries that are cached in the software. The range is from 0 to 1048576. The default value is 8000 entries.
interval <i>seconds</i>	Specifies the maximum time interval before an entry is sent to a syslog. The range is from 5 to 86400. The default value is 300 seconds.
threshold <i>num_packets</i>	Specifies the number of packet matches (hits) before an entry is sent to a syslog. The range is from 0 to 1000000. The default value is 0 packets—rate limiting is off; the system log is not triggered by the number of packet matches.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify the maximum number of log entries that are cached in the software:

```
switch# configure terminal
switch(config)# logging ip access-list cache entries 200
switch(config)#
```

This example shows how to specify the maximum time interval before an entry is sent to the system log:

```
switch# configure terminal
switch(config)# logging ip access-list cache interval 350
switch(config)#
```

Send comments to nexus5k-docfeedback@cisco.com

This example shows how to specify the number of packet matches before an entry is sent to the system log:

```
switch# configure terminal
switch(config)# logging ip access-list cache threshold 125
switch(config)#
```

Related Commands

Command	Description
show logging ip access-list	Displays the status of IP access list logging.

Send comments to nexus5k-docfeedback@cisco.com

logging level

To enable logging messages from a defined facility that have the specified severity level or higher, use the **logging level** command. To disable logging messages from a defined facility, use the **no** form of this command.

logging level *facility severity-level*

no logging level *facility severity-level*

Syntax Description		
<i>facility</i>	Facility. The facilities are listed in Table 1-1 of Appendix 1, "System Message Logging Facilities."	To apply the same severity level to all facilities, use the all facility.
<i>severity-level</i>	Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows:	<ul style="list-style-type: none"> • 0—emergency: System unusable • 1—alert: Immediate action needed • 2—critical: Critical condition—default level • 3—error: Error condition • 4—warning: Warning condition • 5—notification: Normal but significant condition • 6—informational: Informational message only • 7—debugging: Appears during debugging only

Command Default None

Command Modes Global configuration mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.
	5.0(3)N1(1)	Support for multicast and unicast routing features was added.
	5.0(3)N2(1)	Support for Flex Links and Fibre Channel over Ethernet (FCoE) N-Port Virtualizer (NPV) was added.

Examples This example shows how to enable logging messages from the AAA facility that have a severity level of 2 or higher:

```
switch(config)# logging level aaa 2
```

Send comments to nexus5k-docfeedback@cisco.com

Related Commands

Command	Description
show logging level	Displays the facility logging level configuration.

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

logging logfile

To configure the name of the log file used to store system messages and the minimum severity level to log, use the **logging logfile** command. To disable logging to the log file, use the **no** form of this command.

logging logfile *logfile-name severity-level [size bytes]*

no logging logfile [*logfile-name severity-level [size bytes]*]

Syntax Description

<i>logfile-name</i>	Name of the log file to be used to store system messages.
<i>severity-level</i>	Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows: <ul style="list-style-type: none"> • 0—emergency: System unusable • 1—alert: Immediate action needed • 2—critical: Critical condition—default level • 3—error: Error condition • 4—warning: Warning condition • 5—notification: Normal but significant condition • 6—informational: Informational message only • 7—debugging: Appears during debugging only
<i>size bytes</i>	(Optional) Specifies a maximum file size. The default file size is 4194304 bytes and can be configured from 4096 to 4194304 bytes.

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 configure a log file called logfile to store system messages and set its severity level to 4:

```
switch(config)# logging logfile logfile 4
```

Related Commands

Command	Description
show logging logfile	Displays the log file.

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

logging module

To enable module log messages, use the **logging module** command. To disable module log messages, use the **no** form of this command.

logging module [*severity-level*]

no logging module

Syntax Description

<i>severity-level</i>	(Optional) Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows: <ul style="list-style-type: none"> • 0—emergency: System unusable • 1—alert: Immediate action needed • 2—critical: Critical condition • 3—error: Error condition • 4—warning: Warning condition • 5—notification: Normal but significant condition—default level • 6—informational: Informational message only • 7—debugging: Appears during debugging only
-----------------------	---

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

Set a specified severity level or use the default.

Examples

This example shows how to enable module log messages:

```
switch(config)# logging module
```

Related Commands

Command	Description
show logging module	Displays the module logging status.

Send comments to nexus5k-docfeedback@cisco.com

logging monitor

To enable the device to log messages to the monitor (terminal line), use the **logging monitor** command. To disable monitor log messages, use the **no** form of this command.

logging monitor [*severity-level*]

no logging monitor

Syntax Description

severity-level

(Optional) Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows:

- **0**—emergency: System unusable
- **1**—alert: Immediate action needed
- **2**—critical: Critical condition—default level
- **3**—error: Error condition
- **4**—warning: Warning condition
- **5**—notification: Normal but significant condition
- **6**—informational: Informational message only
- **7**—debugging: Appears during debugging only

Command Default

None

Command Modes

Global configuration mode

Command History

Release

Modification

4.0(0)N1(1a)

This command was introduced.

Usage Guidelines

This configuration applies to Telnet and Secure Shell (SSH) sessions.

Examples

This example shows how to enable monitor log messages:

```
switch(config)# logging monitor
```

Related Commands

Command

Description

show logging monitor

Displays the status of monitor logging.

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

logging server

To configure a remote syslog server at the specified hostname or IPv4/IPv6 address, use the **logging server** command. To disable the remote syslog server, use the **no** form of this command.

```
logging server host [severity-level] [facility {auth | authpriv | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | syslog | user | uucp} | use-vrf {vrf_name | management}]
```

```
no logging server host [severity-level] [facility {auth | authpriv | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | syslog | user | uucp} | use-vrf {vrf_name | management}]
```

Syntax Description	
<i>host</i>	Hostname or IPv4/IPv6 address of the remote syslog server.
<i>severity-level</i>	(Optional) Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows: <ul style="list-style-type: none"> • 0—emergency: System unusable • 1—alert: Immediate action needed • 2—critical: Critical condition—default level • 3—error: Error condition • 4—warning: Warning condition • 5—notification: Normal but significant condition • 6—informational: Informational message only • 7—debugging: Appears during debugging only
facility <i>facility</i>	(Optional) Specifies the outgoing <i>facility</i> . The facilities are listed in Table 1-1 of Appendix 1, “System Message Logging Facilities.” The default outgoing facility is local7 .
vrf <i>vrf_name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) to be used in the remote server. The name can be a maximum of 32 alphanumeric characters.
management	Specifies the management VRF. This is the default VRF.

Command Default The default outgoing facility is **local7**.
The default VRF is **management**.

Command Modes Global configuration mode

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.
	4.1(3)N2(1)	The use-vrf keyword was added.

Send comments to nexus5k-docfeedback@cisco.com

Examples

This example shows how to configure a remote syslog server at a specified IPv4 address, using the default outgoing facility:

```
switch(config)# logging server 192.168.2.253
```

This example shows how to configure a remote syslog server at a specified hostname with severity level 5 or higher:

```
switch(config)# logging server syslogA 5
```

Related Commands

Command	Description
show logging server	Displays the configured syslog servers.

Send comments to nexus5k-docfeedback@cisco.com

logging timestamp

To set the logging time-stamp units, use the **logging timestamp** command. To reset the logging time-stamp units to the default, use the **no** form of this command.

logging timestamp { **microseconds** | **milliseconds** | **seconds** }

no logging timestamp { **microseconds** | **milliseconds** | **seconds** }

Syntax Description

microseconds	Specifies the units to use for logging timestamps in microseconds. The default units are seconds .
milliseconds	Specifies the units to use for logging timestamps in milliseconds.
seconds	Specifies the units to use for logging timestamps in seconds. The default units are seconds .

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

By default, the units are seconds.

Examples

This example shows how to set the logging time-stamp units to microseconds:

```
switch(config)# logging timestamp microseconds
```

Related Commands

Command	Description
show logging timestamp	Displays the logging time-stamp configuration.

Send comments to nexus5k-docfeedback@cisco.com



M Commands

This chapter describes the system management commands that begin with M.

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

mtu

To configure the maximum transmission unit (MTU) truncation size for packets in the specified Ethernet Switched Port Analyzer (SPAN) session, use the **mtu** command. To remove the MTU truncation size configuration, use the **no** form of this command.

mtu *mtu-size*

no mtu

Syntax Description

<i>mtu-size</i>	MTU truncation size. The range is from 64 to 1500.
-----------------	--

Command Default

Disabled

Command Modes

Monitor configuration (config-monitor)

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

MTU truncation and the SPAN rate limit cannot be enabled for the same SPAN session. If you configure both for one session, only the rate limit is allowed on F1 Series modules, and MTU truncation is disabled until you disable the rate limit configuration.



Note

MTU truncation is supported only on F1 Series modules and F2 Series modules.

This command does not require a license.

Examples

This example shows how to configure the MTU truncation size for packets in the specified SPAN session:

```
switch# configure terminal
switch(config)# monitor session 5
switch(config-monitor)# mtu 128
switch(config-monitor)#
```

This example shows how to remove the MTU truncation size configuration for packets in the specified SPAN session:

```
switch# configure terminal
```

Send comments to nexus5k-docfeedback@cisco.com

```
switch(config)# monitor session 5  
switch(config-monitor)# no mtu
```

Related Commands

Command	Description
monitor session	Places you in the monitor configuration mode for configuring a SPAN session.
show monitor session	Displays the status of the SPAN session.

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com



N Commands

This chapter describes the system management commands that begin with N.

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

ntp

To configure the Network Time Protocol (NTP) peers and servers for the switch, use the **ntp** command. To remove configured peers and servers, use the **no** form of this command.

```
ntp {peer hostname | server hostname} [prefer] [use-vrf vrf-name]
```

```
no ntp {peer hostname | server hostname}
```

Syntax Description

peer <i>hostname</i>	Specifies the hostname or IP address of an NTP peer.
server <i>hostname</i>	Specifies the hostname or IP address of the NTP server.
prefer	(Optional) Specifies this peer/server as the preferred peer/server.
use-vrf <i>vrf-name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) used to reach this peer/server.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
4.0(1a)N1(1)	The keyword use-vrf replaces the keyword vrf . The keyword vrf is retained for backwards compatibility.

Usage Guidelines

You can specify multiple peer associations.

Examples

This example shows how to form a server association with a server:

```
switch(config)# ntp server ntp.cisco.com
```

This example shows how to form a peer association with a peer:

```
switch(config)# ntp peer 192.168.10.0
```

This example shows how to delete an association with a peer:

```
switch(config)# no ntp peer 192.168.10.0
```

Related Commands

Command	Description
ntp distribute	Enables CFS distribution for NTP.
show ntp	Displays NTP information.

Send comments to nexus5k-docfeedback@cisco.com

ntp abort

To discard the Network Time Protocol (NTP) Cisco Fabric Services (CFS) distribution session in progress, use the **ntp abort** command.

ntp abort

Syntax Description This command has no arguments or keywords.

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 discard the NTP CFS distribution session in progress:

```
switch(config)# ntp abort
```

Related Commands	Command	Description
	ntp distribute	Enables CFS distribution for NTP.
	show ntp	Displays NTP information.

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

ntp authenticate

To enable Network Time Protocol (NTP) authentication, use the `ntp authenticate` command. To disable NTP authentication, use the `no` form of this command.

ntp authenticate

no ntp authenticate

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration (config)

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

Usage Guidelines This command does not require a license.

Examples This example shows how to enable NTP authentication:

```
switch(config)# ntp authenticate
```

This example shows how to disable NTP authentication:

```
switch(config)# no ntp authenticate
switch(config)#
```

Related Commands	Command	Description
	<code>show ntp authentication-status</code>	Displays the status of NTP authentication.

Send comments to nexus5k-docfeedback@cisco.com

ntp commit

To apply the pending configuration pertaining to the Network Time Protocol (NTP) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **ntp commit** command.

ntp commit

Syntax Description This command has no arguments or keywords.

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 commit changes to the active NTP configuration:

```
switch(config)# ntp commit
```

Related Commands	Command	Description
	ntp distribute	Enables CFS distribution for NTP.
	show ntp	Displays NTP information.

Send comments to nexus5k-docfeedback@cisco.com

ntp distribute

To enable Cisco Fabric Services (CFS) distribution for Network Time Protocol (NTP), use the **ntp distribute** command. To disable this feature, use the **no** form of this command.

ntp distribute

no ntp distribute

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 Before distributing the Fibre Channel timer changes to the fabric, the temporary changes to the configuration must be committed to the active configuration using the **ntp commit** command.

Examples This example shows how to distribute the active NTP configuration to the fabric:

```
switch(config)# ntp distribute
```

Related Commands	Command	Description
	ntp commit	Commits the NTP configuration changes to the active configuration.
	show ntp	Displays NTP information.

Send comments to nexus5k-docfeedback@cisco.com

ntp sync-retry

To retry synchronization with the configured Network Time Protocol (NTP) servers, use the **ntp sync-retry** command.

ntp sync-retry

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 retry synchronization with the configured NTP servers:

```
switch# ntp sync-retry
```

Related Commands	Command	Description
	ntp distribute	Enables CFS distribution for NTP.
	show ntp	Displays NTP information.

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com



P Commands

This chapter describes the system management commands that begin with P.

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

poweroff module

To power off a module, use the **poweroff module** command. To return power to the module, use the **no** form of this command.

poweroff module *module*

no poweroff module *module*

Syntax Description	<i>module</i>	Module number. The range is from 1 to 18.
Defaults	None	
Command Default	Global configuration (config)	
SupportedUserRoles	network-admin vdc-admin	
Command History	Release	Modification
	5.0(3)	The command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example shows how to power off module 2: switch# poweroff module 2	
Related Commands	Command	Description
	show module	Displays information about modules.

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

ptp announce

To configure the interval between PTP announcement messages on an interface or the number of PTP intervals before a timeout occurs on an interface, use the **ptp announce** command. To disable this feature, use the **no** form of this command.

```
ptp announce {interval log-seconds | timeout count}
```

```
no ptp announce
```

Syntax Description

interval <i>log-seconds</i>	The number of log seconds between PTP announcement messages. The range is from 0 to 4 seconds.
timeout <i>count</i>	The number of PTP intervals before a timeout occurs on the interface. The range is from 2 to 10.

Command Default

The default interval is 1 log second.
The default timeout is 3 announce intervals.

Command Modes

Interfaces configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to set the announcement interval on interface 5/1 to 1:

```
switch# configure terminal
switch(config) # interface ethernet 5/1
switch(config-if) # ptp announce interval 1
switch(config-if)
```

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the device.
ptp delay request minimum interval	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.
ptp sync interval	Configures the interval between PTP synchronization messages on an interface.
ptp vlan	Configures the VLAN for the interface where PTP is being enabled.
show ptp brief	Displays the PTP status.
show ptp port interface ethernet	Displays the status of the PTP port on the switch.

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

ptp delay request minimum interval

To configure the minimum interval allowed between PTP delay request messages when the port is in the master state, use the **ptp delay request minimum interval** command. To disable this feature, use the **no** form of this command.

ptp delay request minimum interval *log-seconds*

no ptp delay request minimum interval

Syntax Description	<i>log-seconds</i>	The number of log seconds between PTP delay request messages. The range is from -1 to 6 seconds.
--------------------	--------------------	--

Command Default	0 log seconds
-----------------	---------------

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

Command History	Release	Modification
	5.2(1)N1(1)	This command was introduced.

Examples This example shows how to set the minimum delay request interval to 3:

```
switch# configure terminal
switch(config) # interface ethernet 5/1
switch(config-if) # ptp delay request minimum interval 3
```

Related Commands	Command	Description
	feature ptp	Enables or disables PTP on the device.
	ptp announce	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.
	ptp sync interval	Configures the interval between PTP synchronization messages on an interface.
	ptp vlan	Configures the VLAN for the interface where PTP is being enabled.
	show ptp brief	Displays the PTP status.
	show ptp port interface ethernet	Displays the status of the PTP port on the switch.

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

ptp domain

To configure the domain number to use for this clock, use the **ptp domain** command. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network.

ptp domain *number*

no ptp domain *number*

Syntax Description	<i>number</i>	Configures the domain number to use for this clock. The range is from 0 to 128.
--------------------	---------------	---

Command Default	0
-----------------	---

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

Command History	Release	Modification
	5.2(1)N1(1)	This command was introduced.

Examples This example shows how to configure the domain number for use with a clock:

```
switch(config)# ptp domain 1
```

Related Commands	Command	Description
	feature ptp	Enables or disables PTP on the device.
	ptp source	Configures the source IP address for all PTP packets.
	ptp priority1	Configures the priority 1 value to use when advertising this clock.
	ptp priority2	Configures the priority 1 value to use when advertising this clock.
	show ptp brief	Displays the PTP status.
	show ptp clock	Displays the properties of the local clock.

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

ptp priority1

To configure the priority1 value to use when advertising this clock, use the **ptp priority1** command.

ptp priority1 *value*

no ptp priority1 *value*

Syntax Description

<i>value</i>	The configured value overrides the default criteria (clock quality, clock class, etc.) for best master clock selection. Lower values take precedence. The range is from 0 to 255.
--------------	---

Command Default

255 when advertising the clock

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to set the priority1 value used to advertise this clock:

```
switch(config)# ptp priority1 10
```

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the device.
ptp source	Configures the source IP address for all PTP packets.
ptp domain	Configures the domain number to use for this clock.
ptp priority2	Configures the priority2 value to use when advertising this clock.
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.

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

ptp priority2

To configure the priority2 value to use when advertising this clock, use the **ptp priority2** command.

ptp priority2 *value*

no ptp priority2 *value*

Syntax Description

<i>value</i>	The configured value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255.
--------------	---

Command Default

255 when advertising the clock

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to set the priority2 value used to advertise this clock:

```
switch(config)# ptp priority2 20
```

Related Commands

Command	Description
feature ptp	Enables or disables PTP on the device.
ptp source	Configures the source IP address for all PTP packets.
ptp domain	Configures the domain number to use for this clock.
ptp priority1	Configures the priority1 value to use when advertising this clock.
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.

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

ptp source

To configure the source IP address for all PTP packets, use the **ptp source** command. To unconfigure the source IP address for all PTP packets, use the **no** form of this command.

ptp source *ip-address* [**vrf** *vrf*]

no ptp source *ip-address* [**vrf** *vrf*]

Syntax Description		
	<i>ip-address</i>	Specifies the source IP address for all PTP packets. The IP address can be in IPv4 or IPv6 format.
	vrf <i>vrf</i>	Specifies the VRF.

Command Default None

Command Modes Global configuration mode

Command History	Release	Modification
	5.2(1)N1(1)	This command was introduced.

Examples This example shows how to configure the source IP address for all PTP packets:

```
switch(config)# ptp source 192.0.2.1
```

Related Commands	Command	Description
	feature ptp	Enables or disables PTP on the device.
	ptp domain	Configures the domain number to use for this clock.
	ptp priority1	Configures the priority 1 value to use when advertising this clock.
	ptp priority2	Configures the priority 1 value to use when advertising this clock.
	show ptp brief	Displays the PTP status.
	show ptp clock	Displays the properties of the local clock.

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

ptp sync interval

To configure the interval between PTP synchronization messages, use the **ptp sync interval** command. To disable this feature, use the **no** form of this command.

ptp sync interval *log-seconds*

no ptp sync interval

Syntax Description	<i>log-seconds</i>	The number of log seconds between PTP synchronization messages on an interface. The range is from -3 seconds to 1 second.
---------------------------	--------------------	---

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

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

Command History	Release	Modification
	5.2(1)N1(1)	This command was introduced.

Examples This example shows how to set the PTP synchronization interval to -3:

```
switch# configure terminal
switch(config) # interface ethernet 5/1
switch(config-if) # ptp sync interval -3
```

Related Commands	Command	Description
	feature ptp	Enables or disables PTP on the device.
	ptp announce	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.
	ptp delay request minimum interval	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.
	ptp vlan	Configures the VLAN for the interface where PTP is being enabled.
	show ptp brief	Displays the PTP status.
	show ptp port interface ethernet	Displays the status of the PTP port on the switch.

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

ptp vlan

To specify the VLAN for the interface where PTP is being enabled, use the **ptp vlan** command. To disable this feature, use the **no** form of this command.

ptp vlan *vlan-id*

no ptp vlan

Syntax Description	<i>vlan-id</i>	The VLAN ID for the interface where PTP is being enabled. The range is from 1 to 4094.
Command Default	1	
Command Modes	Interface configuration mode	
Command History	Release	Modification
	5.2(1)N1(1)	This command was introduced.
Usage Guidelines	PTP can only be enabled on one VLAN on an interface.	
Examples	This example shows how to specify VLAN 10 as the interface where PTP is being enabled:	
	<pre>switch# configure terminal switch(config) # interface ethernet 5/1 switch(config-if) # ptp vlan 10</pre>	
Related Commands	Command	Description
	feature ptp	Enables or disables PTP on the device.
	ptp announce	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.
	ptp delay request minimum interval	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.
	ptp sync interval	Configures the interval between PTP synchronization messages on an interface.
	show ptp brief	Displays the PTP status.
	show ptp port interface ethernet	Displays the status of the PTP port on the switch.

Send comments to nexus5k-docfeedback@cisco.com



S Commands

This chapter describes the system management commands that begin with S.

Send comments to nexus5k-docfeedback@cisco.com

shut (ERSPAN)

To shut down an Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **shut** command. To enable an ERSPAN session, use the **no** form of this command.

shut

no shut

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes ERSPAN session configuration 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 shut down an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# shut
switch(config-erspan-src)#
```

This example shows how to enable an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# no shut
switch(config-erspan-src)#
```

Related Commands	Command	Description
	monitor session	Enters the monitor configuration mode.
	show monitor session	Displays the virtual SPAN or ERSPAN configuration.

Send comments to nexus5k-docfeedback@cisco.com

snmp-server community

To create Simple Network Management Protocol (SNMP) communities for SNMPv1 or SNMPv2c, use the **snmp-server community** command. To revert to the defaults, use the **no** form of this command.

```
snmp-server community com-name [group grp-name | ro | rw | use-acl acl-name]
```

```
no snmp-server community com-name [group grp-name | ro | rw | use-acl acl-name]
```

Syntax Description	
<i>com-name</i>	SNMP community string. The name can be any alphanumeric string up to 32 characters.
group <i>grp-name</i>	(Optional) Specifies the group to which the community belongs. The name can be a maximum of 32 characters.
ro	(Optional) Specifies read-only access with this community string.
rw	(Optional) Specifies read-write access with this community string.
use-acl <i>acl-name</i>	(Optional) Specifies the access control list (ACL) to filter SNMP requests. The name can be a maximum of 32 characters.

Command Default None

Command Modes Global configuration mode

Command History	Release	Modification
	5.2(1)N1(1)	IPv6 support added.
	4.2(1)N1(1)	This command was introduced.

Usage Guidelines You can assign an access list (ACL) to a community to filter incoming SNMP requests. If the assigned ACL allows the incoming request packet, SNMP processes the request. If the ACL denies the request, SNMP drops the request and sends a system message.

See the *Cisco Nexus 5000 Series NX-OS Security Configuration Guide* for more information on creating ACLs. The ACL applies to both IPv4 and IPv6 over UDP and TCP. After creating the ACL, assign the ACL to the SNMP community.

Examples This example shows how to create an SNMP community string and assign an ACL to the community to filter SNMP requests:

```
switch(config)# snmp-server community public use-acl my_acl_for_public
switch(config)#
```

Related Commands

Send comments to nexus5k-docfeedback@cisco.com

Command	Description
<code>show snmp community</code>	Displays the SNMP community strings.

Send comments to nexus5k-docfeedback@cisco.com

snmp-server contact

To configure the Simple Network Management Protocol (SNMP) contact (sysContact) information, use the **snmp-server contact** command. To remove the contact information, use the **no** form of this command.

```
snmp-server contact [text]
```

```
no snmp-server contact [text]
```

Syntax Description	<i>text</i>	(Optional) String that describes the system contact information. The text can be any alphanumeric string up to 32 characters and cannot contain spaces.
---------------------------	-------------	---

Command Default	No system contact (sysContact) string is set.
------------------------	---

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

Command History	Release	Modification
	4.1(3)N2(1)	This command was introduced.

Examples	This example shows how to set an SNMP contact:
	<pre>switch(config)# snmp-server contact DialSystemOperatorAtBeeper#1235 switch(config)#</pre>
	This example shows how to remove an SNMP contact:
	<pre>switch(config)# no snmp-server contact DialSystemOperatorAtBeeper#1235 switch(config)#</pre>

Related Commands	Command	Description
	show snmp	Displays information about SNMP.
	snmp-server location	Sets the system location string.

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

snmp-server context

To configure the Simple Network Management Protocol (SNMP) context to logical network entity mapping, use the **snmp-server context** command. To remove the context, use the **no** form of this command.

```
snmp-server context context-name [instance instance-name] [vrf {vrf-name | default | management}] [topology topology-name]
```

```
no snmp-server context context-name [instance instance-name] [vrf {vrf-name | default | management}] [topology topology-name]
```

Syntax Description

<i>context-name</i>	SNMP context. The name can be any alphanumeric string up to 32 characters.
instance <i>instance-name</i>	(Optional) Specifies a protocol instance. The name can be any alphanumeric string up to 32 characters.
vrf <i>vrf-name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) instance. The name is case sensitive, and can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.
topology <i>topology-name</i>	(Optional) Specifies the topology. The name can be any alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.1(3)N2(1)	This command was introduced.

Usage Guidelines

Use the **snmp-server context** command to map between SNMP contexts and logical network entities, such as protocol instances or VRFs.

Examples

This example shows how to map the public1 context to the default VRF:

```
switch(config)# snmp-server context public1 vrf default
switch(config)#
```

Send comments to nexus5k-docfeedback@cisco.com

Related Commands	Command	Description
	show snmp	Displays the SNMP status.
	show snmp context	Displays information about SNMP contexts.

Send comments to nexus5k-docfeedback@cisco.com

snmp-server enable traps

To enable the Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps** command. To disable SNMP notifications, use the **no** form of this command.

snmp-server enable traps

```
[aaa [server-state-change] |
callhome [event-notify | smtp-send-fail] |
entity {entity_fan_status_change | entity_mib_change | entity_module_inserted |
entity_module_removed | entity_module_status_change | entity_power_out_change |
entity_power_status_change | entity_unrecognised_module} |
fcdomain |
fcns |
fcs |
fctrace |
fspf |
license [notify-license-expiry | notify-license-expiry-warning | notify-licensefile-missing |
notify-no-license-for-feature] |
link |
rf [redundancy_framework] |
rmon [fallingAlarm | hcFallingAlarm | hcRisingAlarm | risingAlarm] |
rscn |
snmp [authentication] |
stpx {inconsistency | loop-inconsistency | root-inconsistency} |
vsan | vtp |
zone [default-zone-behavior-change | merge-failure | merge-success | request-reject1 |
unsupp-mem]]
```

no snmp-server enable traps

```
[aaa [server-state-change] |
callhome [event-notify | smtp-send-fail] |
entity {entity_fan_status_change | entity_mib_change | entity_module_inserted |
entity_module_removed | entity_module_status_change | entity_power_out_change |
entity_power_status_change | entity_unrecognised_module} |
fcdomain |
fcns |
fcs |
fctrace |
fspf |
license [notify-license-expiry | notify-license-expiry-warning | notify-licensefile-missing |
notify-no-license-for-feature] |
link |
rf [redundancy_framework] |
rmon [fallingAlarm | hcFallingAlarm | hcRisingAlarm | risingAlarm] |
rscn |
snmp [authentication] |
stpx {inconsistency | loop-inconsistency | root-inconsistency} |
vsan | vtp |
zone [default-zone-behavior-change | merge-failure | merge-success | request-reject1 |
unsupp-mem]]
```


Send comments to nexus5k-docfeedback@cisco.com

Syntax	Description
aaa	(Optional) Enables notifications for a AAA server state change.
server-state-change	(Optional) Specifies the AAA server state change.
callhome	(Optional) Enables Cisco Call Home notifications.
event-notify	(Optional) Specifies the Cisco Call Home external event notification.
smtp-send-fail	(Optional) Specifies the SMTP message send fail notification.
entity	(Optional) Enables notifications for a change in the module status, fan status, or power status.
entity_fan_status_change	(Optional) Specifies the entity fan status change.
entity_mib_change	(Optional) Specifies the entity MIB change.
entity_module_inserted	(Optional) Specifies the entity module inserted.
entity_module_removed	(Optional) Specifies the entity module removed.
entity_module_status_change	(Optional) Specifies the entity module status change.
entity_power_out_change	(Optional) Specifies the entity power out change.
entity_power_status_change	(Optional) Specifies the entity power status change.
entity_unrecognised_module	(Optional) Specifies the entity unrecognized module.
fdomain	(Optional) Enables notifications for the Fibre Channel domain.
fcns	(Optional) Enables notifications for the name server.
fc	(Optional) Enables notifications for the fabric configuration server.
fctrace	(Optional) Enables notifications for the route to an N port.
fspf	(Optional) Enables notifications for the Fabric Shortest Path First (FSPF).
license	(Optional) Enables notifications for the license manager.
notify-license-expiry	(Optional) Specifies the license expiry notification.
notify-license-expiry-warning	(Optional) Specifies the license expiry warning notification.
notify-licensefile-missing	(Optional) Specifies the license file missing notification.
notify-no-license-for-feature	(Optional) Specifies that a notification is sent when no license needs to be installed for the feature.
link	(Optional) Enables notifications for uplink and downlink interfaces.
rf	(Optional) Enables notifications for the redundancy framework.
redundancy_framework	(Optional) Specifies the Redundancy_Framework (RF) supervisor switchover MIB.
rmon	(Optional) Enables notifications for rising, falling, and high-capacity alarms.
fallingAlarm	(Optional) Specifies the RMON falling alarm.
hcFallingAlarm	(Optional) Specifies the high-capacity RMON falling alarm.
hcRisingAlarm	(Optional) Specifies the high-capacity RMON rising alarm.

Send comments to nexus5k-docfeedback@cisco.com

risingAlarm	(Optional) Specifies the RMON rising alarm.
rscn	(Optional) Enables RSCN notifications.
snmp	(Optional) Enables SNMP authentication notifications.
authentication	(Optional) Specifies the SNMP authentication trap.
vsan	(Optional) Enables notifications for VSANs.
vtp	(Optional) Enables notifications for a VLAN Trunking Protocol (VTP) domain.
zone	(Optional) Enables zone notifications.
default-zone-behavior-change	(Optional) Specifies the default zone behavior change notification.
merge-failure	(Optional) Specifies the merge failure notification.
merge-success	(Optional) Specifies the merge success notification.
request-reject1	(Optional) Specifies the request reject notification.
unsupp-mem	(Optional) Specifies the unsupported member notification.
stp	(Optional) Enables STPX MIB notifications.
inconsistency	(Optional) Enables SNMP STPX MIB InconsistencyUpdate notifications.
loop-inconsistency	(Optional) Enables SNMP STPX MIB Loop InconsistencyUpdate notifications.
root-inconsistency	(Optional) Enables SNMP STPX MIB RootInconsistencyUpdate notifications.

Command Default

All notifications

Command Modes

Global configuration mode

Command History

Release	Modification
4.1(3)N2(1)	This command was introduced.
5.0(2)N1(1)	Added support to enable SNMP traps for a VLAN Trunking Protocol (VTP) domain.

Usage Guidelines

The **snmp-server enable traps** command enables both traps and informs, depending on the configured notification host receivers.

Examples

This example shows how to enable SNMP notifications for the server state change:

```
switch(config)# snmp-server enable traps aaa
switch(config)#
```

This example shows how to disable all SNMP notifications:

```
switch(config)# no snmp-server enable traps
switch(config)#
```

Send comments to nexus5k-docfeedback@cisco.com

Related Commands	Command	Description
	snmp-server enable traps link	Enables the Simple Network Management Protocol (SNMP) notifications on link traps.
	show snmp trap	Displays the SNMP notifications enabled or disabled.

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

snmp-server enable traps link

To enable the Simple Network Management Protocol (SNMP) notifications on link traps, use the **snmp-server enable traps link** command. To disable SNMP notifications on link traps, use the **no** form of this command.

snmp-server enable traps link [*notification-type*]

no snmp-server enable traps link [*notification-type*]

Syntax Description	<i>notification-type</i>	<p>(Optional) Type of notification to enable. If no type is specified, all notifications available on your device are sent. The notification type can be one of the following keywords:</p> <ul style="list-style-type: none"> • IETF-extended-linkDown—Enables the Internet Engineering Task Force (IETF) extended link state down notification. • IETF-extended-linkUp—Enables the IETF extended link state up notification. • cisco-extended-linkDown—Enables the Cisco extended link state down notification. • cisco-extended-linkUp—Enables the Cisco extended link state up notification. • connUnitPortStatusChange—Enables the overall status of the connectivity unit Notification. • delayed-link-state-change—Enables the delayed link state change. • fcTrunkIfDownNotify—Enables the Fibre Channel Fabric Element (FCFE) link state down notification. • fcTrunkIfUpNotify—Enables the FCFE link state up notification. • fcot-inserted—Specifies that the Fibre Channel optical transmitter (FCOT) hardware has been inserted. • fcot-removed—Specifies that the FCOT has been removed. • linkDown—Enables the IETF Link state down notification. • linkUp—Enables the IETF Link state up notification.
---------------------------	--------------------------	--

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

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

Command History	Release	Modification
	4.1(3)N2(1)	This command was introduced.

Send comments to nexus5k-docfeedback@cisco.com

Usage Guidelines

This command is disabled by default. Most notification types are disabled.

If you enter this command with no *notification-type* arguments, the default is to enable all notification types controlled by this command

Examples

This example shows how to enable the SNMP link trap notification on the switch:

```
switch(config)# snmp-server enable traps link  
switch(config)#
```

This example shows how to disable the SNMP link trap notification on the switch:

```
switch(config)# no snmp-server enable traps link  
switch(config)#
```

Related Commands

Command	Description
show snmp trap	Displays the SNMP notifications enabled or disabled.

Send comments to nexus5k-docfeedback@cisco.com

snmp-server globalEnforcePriv

To configure Simple Network Management Protocol (SNMP) message encryption for all users, use the **snmp-server globalEnforcePriv** command. To remove the encryption, use the **no** form of this command.

snmp-server globalEnforcePriv

no snmp-server globalEnforcePriv

Syntax Description This command has no arguments or keywords.

Command Default The SNMP agent accepts SNMPv3 messages without authentication and encryption.

Command Modes Global configuration mode

Command History	Release	Modification
	4.1(3)N2(1)	This command was introduced.

Examples This example shows how to configure SNMP message encryption for all users:

```
switch(config)# snmp-server globalEnforcePriv
switch(config)#
```

This example shows how to remove SNMP message encryption for all users:

```
switch(config)# no snmp-server globalEnforcePriv
switch(config)#
```

Related Commands	Command	Description
	snmp-server user	Configures a new user to an SNMP group.
	show snmp sessions	Displays the current SNMP sessions.

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

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command. To remove the specified host, use the **no** form of this command.

```
snmp-server host host-address { community-string
| filter-vrf { vrf-name | default | management }
| { informs | traps } { community-string | version { 1 | 2c | 3 { auth | noauth | priv } }
community-string [udp-port port]}
| version { 1 | 2c | 3 { auth | noauth | priv } } community-string [udp-port port]}

```

```
no snmp-server host host-address { community-string
| filter-vrf { vrf-name | default | management }
| { informs | traps } { community-string | version { 1 | 2c | 3 { auth | noauth | priv } }
community-string [udp-port port]}
| version { 1 | 2c | 3 { auth | noauth | priv } } community-string [udp-port port]}

```

Syntax Description

<i>host-address</i>	IPv4 or IPv6 address or DNS name of the SNMP notification host.
<i>community-string</i>	String sent with the notification operation. The string can be a maximum of 32 alphanumeric characters. We recommend that you define this string using the snmp-server community command prior to using the snmp-server host command.
filter-vrf <i>vrf-name</i>	Specifies the virtual routing and forwarding (VRF) instance. The name is case sensitive and can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.
informs	Sends SNMP informs to this host.
traps	Sends SNMP traps to this host.
version	Specifies the version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the priv keyword. If you use the version keyword, one of the following must be specified: <ul style="list-style-type: none"> • 1—SNMPv1. • 2c—SNMPv2C. • 3—SNMPv3. The following three optional keywords can follow the version 3 keyword: <ul style="list-style-type: none"> – auth—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication – noauth (Default)—The noAuthNoPriv security level. This is the default if the auth, noauth, or priv keyword is not specified. – priv—Enables Data Encryption Standard (DES) packet encryption (also called “privacy”)
udp-port <i>port</i>	(Optional) Specifies the UDP port of the host to use. The port range is from 0 to 65535.

Send comments to nexus5k-docfeedback@cisco.com

Command Default Disabled

Command Modes Global configuration mode

Command History	Release	Modification
	5.2(1)N1(1)	IPv6 support added.
	4.1(3)N2(1)	This command was introduced.

Usage Guidelines SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Therefore, informs are more likely to reach their intended destination.

Examples This example shows how to send the SNMP traps to the host specified by the IPv4 address 192.168.0.10. The community string is defined as my_acl_for_public.:

```
switch(config)# snmp-server community public use-acl my_acl_for_public
switch(config)# snmp-server host 192.168.0.10 my_acl_for_public
switch(config)#
```

This example shows how to send all inform requests to the host myhost.cisco.com using the community string my_acl_for_public:

```
switch(config)# snmp-server enable traps
switch(config)# snmp-server host myhost.cisco.com informs version 2c my_acl_for_public
switch(config)#
```

Related Commands	Command	Description
	show snmp host	Displays information about the SNMP host.

Send comments to nexus5k-docfeedback@cisco.com

snmp-server location

To set the Simple Network Management Protocol (SNMP) system location string, use the **snmp-server location** command. To remove the location string, use the **no** form of this command.

snmp-server location *text*

no snmp-server location *text*

Syntax Description	<i>text</i>	(Optional) String that describes the system location information.
--------------------	-------------	---

Command Default	No system location string is set.
-----------------	-----------------------------------

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

Command History	Release	Modification
	4.1(3)N2(1)	This command was introduced.

Examples	This example shows how to set a system location string:
----------	---

```
switch(config)# snmp-server location Building 3/Room 21
switch(config)#
```

Examples	This example shows how to remove the system location string:
----------	--

```
switch(config)# no snmp-server location Building 3/Room 21
switch(config)#
```

Related Commands	Command	Description
	snmp-server contact	Sets the SNMP system contact (sysContact) string.

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

snmp-server mib community-map

To configure a Simple Network Management Protocol (SNMP) context to map to a logical network entity, such as a protocol instance or VRF, use the **snmp-server mib community-map** command. To remove the mapping, use the **no** form of this command.

snmp-server mib community-map *community-string* **context** *context-name*

no snmp-server mib community-map *community-string* **context** *context-name*

Syntax Description

<i>community-string</i>	String sent with the notification operation. The string can be a maximum of 32 alphanumeric characters. We recommend that you define this string using the snmp-server community command prior to using the snmp-server mib community-map command.
context	Specifies the SNMP context to be mapped to the logical network entity.
<i>context-name</i>	SNMP context. The name can be any alphanumeric string up to 32 characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.1(3)N2(1)	This command was introduced.

Examples

This example shows how to map an SNMPv2c community named `my_acl_for_public` to an SNMP context `public1`:

```
switch(config)# snmp-server mib community-map my_acl_for_public context public1
switch(config)#
```

This example shows how to remove the mapping of an SNMPv2c community to an SNMP context:

```
switch(config)# no snmp-server mib community-map my_acl_for_public context public1
switch(config)#
```

Related Commands

Command	Description
snmp-server community	Configures an SNMP community.
snmp-server context	Configures an SNMP context.
show snmp	Displays the SNMP status.

Send comments to nexus5k-docfeedback@cisco.com

snmp-server tcp-session

To enable a one-time authentication for Simple Network Management Protocol (SNMP) over a TCP session, use the **snmp-server tcp-session** command. To disable the one-time authentication, use the **no** form of this command.

snmp-server tcp-session [auth]

no snmp-server tcp-session [auth]

Syntax Description	auth	(Optional) Specifies that one-time authentication for SNMP be enabled over the TCP session.
---------------------------	-------------	---

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

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

Command History	Release	Modification
	4.1(3)N2(1)	This command was introduced.

Examples This example shows how to enable one-time authentication for SNMP over a TCP session:

```
switch(config)# snmp-server tcp-session auth
switch(config)#
```

This example shows how to disable one-time authentication for SNMP over a TCP session:

```
switch(config)# no snmp-server tcp-session auth
switch(config)#
```

Related Commands	Command	Description
	show snmp	Displays the SNMP status.

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

snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the **snmp-server user** command. To remove a user from an SNMP group, use the **no** form of this command.

```
snmp-server user username [groupname] [auth {md5 | sha} auth-password [{engineID engine-ID
| localizedkey | priv {priv-password | aes-128} }]]
```

```
no snmp-server user
```

Syntax Description

<i>username</i>	Name of the user on the host that connects to the agent. The name can be a maximum of 32 alphanumeric characters.
<i>groupname</i>	(Optional) Name of the group to which the user is associated. The name can be a maximum of 32 alphanumeric characters.
auth	(Optional) Specifies that an authentication level setting will be initiated for the session.
md5	(Optional) Specifies that the HMAC-MD5-96 authentication level be used for the session.
sha	(Optional) Specifies that the HMAC-SHA-96 authentication level be used for the session.
<i>auth-password</i>	(Optional) Authentication password for the user that enables the agent to receive packets from the host. The password can be a maximum of 130 characters.
engineID <i>engine-ID</i>	(Optional) Specifies the SNMP engine ID.
localizedkey	(Optional) Specifies whether the passwords are in localized key format.
priv	(Optional) The option that initiates a privacy authentication level setting session.
<i>priv-password</i>	(Optional) Privacy password for the user that enables the host to encrypt the content of the message that it sends to the agent. The password can be a maximum of 130 characters.
aes-128	(Optional) Specifies that a 128-bit AES algorithm for privacy be used for the session.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
4.1(3)N2(1)	This command was introduced.

Examples

This example shows how to configure an SNMP user named authuser with authentication and privacy parameters:

Send comments to nexus5k-docfeedback@cisco.com

```
switch(config)# snmp-server user authuser publicsecurity auth sha shapwd priv aes-128
switch(config)#
```

This example shows how to delete an SNMP user:

```
switch(config)# no snmp-server user authuser
switch(config)#
```

Related Commands

Command	Description
<code>show snmp user</code>	Displays information about one or more SNMP users.

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

snmp trap link-status

To enable Simple Network Management Protocol (SNMP) link trap generation on an interface, use the **snmp trap link-status** command. To disable SNMP link traps, use the **no** form of this command.

snmp trap link-status

no snmp trap link-status

Syntax Description This command has no arguments or keywords.

Command Default Enabled

Command Modes Interface configuration mode
Virtual Ethernet interface configuration mode

Command History	Release	Modification
	4.0(0)N1(1)	This command was introduced.
	5.0(3)N1(1)	Support for Layer 3 interfaces was added.
	5.1(3)N1(1)	Support for virtual Ethernet interfaces was added.

Usage Guidelines By default, SNMP link traps are sent when a Layer 2 interface goes up or down. You can disable SNMP link trap notifications on an individual interface. You can use these limit notifications on a flapping interface (an interface that transitions between up and down repeatedly).

You can use this command on the following interfaces:

- Layer 2 interface
- Layer 3 interface



Note Use the **no switchport** command to configure an interface as a Layer 3 interface.

- Virtual Ethernet interface

Examples This example shows how to disable SNMP link-state traps for a specific Layer 2 interface:

```
switch(config)# interface ethernet 1/1
switch(config-if)# no snmp trap link-status
switch(config-if)#
```

This example shows how to enable SNMP link-state traps for a specific Layer 3 interface:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# snmp trap link-status
```

Send comments to nexus5k-docfeedback@cisco.com

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

This example shows how to enable SNMP link-state traps for a specific Layer 2 interface:

```
switch(config)# interface ethernet 1/1  
switch(config-if)# snmp trap link-status  
switch(config-if)#
```

This example shows how to enable SNMP link-state traps for a specific virtual Ethernet interface:

```
switch(config)# interface vethernet 1  
switch(config-if)# snmp trap link-status  
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
no switchport	Configures an interface as a Layer 3 routed interface.
show snmp trap	Displays the SNMP notifications, enabled or disabled.

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

source (SPAN, ERSPAN)

To add an Ethernet Switched Port Analyzer (SPAN) or an Encapsulated Remote Switched Port Analyzer (ERSPAN) source port, use the **source** command. To remove the source SPAN or ERSPAN port, use the **no** form of this command.

```
source {interface {ethernet slot/port | port-channel channel-num | vethernet veth-num} [{both | rx | tx}] | vlan vlan-num | vsan vsan-num}
```

```
no source {interface {ethernet slot/port | port-channel channel-num | vethernet veth-num} | vlan vlan-num | vsan vsan-num}
```

Syntax Description

interface	Specifies the interface type to use as the source SPAN port.
ethernet <i>slot/port</i>	Specifies the Ethernet interface to use as the source SPAN port. The slot number is from 1 to 255 and the port number is from 1 to 128.
port-channel <i>channel-num</i>	Specifies the EtherChannel interface to use as the source SPAN port. The EtherChannel number is from 1 to 4096.
vethernet <i>veth-num</i>	Specifies the virtual Ethernet interface to use as the source SPAN or ERSPAN port. The virtual Ethernet interface number is from 1 to 1048575.
both	(Optional) Specifies both ingress and egress traffic on the source port. Note This keyword applies to the ERSPAN source port.
rx	(Optional) Specifies only ingress traffic on the source port. Note This keyword applies to the ERSPAN source port.
tx	(Optional) Specifies only egress traffic on the source port. Note This keyword applies to the ERSPAN source port.
vlan <i>vlan-num</i>	Specifies the VLAN interface to use as the source SPAN port. The range is from 1 to 3967 and 4048 to 4093.
vsan <i>vsan-num</i>	Specifies the virtual storage area network (VSAN) to use as the source SPAN port. The range is from 1 to 4093.

Command Default

None

Command Modes

SPAN session configuration mode
ERSPAN session configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.
5.0(2)N1(1)	Port Channel and SAN Port Channel interfaces can be configured as ingress or egress source ports. The limit on the number of egress (TX) sources in a monitor session has been lifted.
5.1(3)N1(1)	Support for a virtual Ethernet interface and ERSPAN was added.

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

Usage Guidelines

A source port (also called a *monitored port*) is a switched port that you monitor for network traffic analysis. In a single local SPAN session, you can monitor source port traffic such as received (Rx), transmitted (Tx), or bidirectional (both).

A source port can be an Ethernet port, port channel, SAN port channel, VLAN, or a VSAN port. It cannot be a destination port.



Note

For Cisco NX-OS Release 4.2(1)N2(1) and earlier, the Cisco Nexus 5010 Switch and the Cisco Nexus 5020 Switch supports a maximum of two egress SPAN source ports.

Beginning with Cisco NX-OS Release 5.0(2)N2(1):

- There is no limit to the number of egress SPAN source ports.
- SAN Port Channel interfaces can be configured as ingress or egress source ports.
- The limit on the number of egress (TX) sources in a monitor session has been lifted.
- Port-channel interfaces can be configured as egress sources.

For ERSPAN, if you do not specify **both**, **rx**, or **tx**, the source traffic is analyzed for both directions.

Examples

This example shows how to configure an Ethernet SPAN source port:

```
switch# configure terminal
switch(config)# monitor session 9 type local
switch(config-monitor)# description A Local SPAN session
switch(config-monitor)# source interface ethernet 1/1
switch(config-monitor)#
```

This example shows how to configure a port channel SPAN source:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface port-channel 5
switch(config-monitor)#
```

This example shows how to configure an ERSPAN source port to receive traffic on the port:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# source interface ethernet 1/5 rx
switch(config-erspan-src)#
```

Related Commands

Command	Description
destination (SPAN, ERSPAN)	Configures a destination SPAN port.
monitor session	Creates a new SPAN session configuration.
show monitor session	Displays SPAN session configuration information.
show running-config monitor	Displays the running configuration information of a SPAN session.

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

switchport monitor rate-limit

To configure a rate limit to monitor traffic on an interface, use the **switchport monitor rate-limit** command. To remove a rate limit, use the **no** form of this command.

switchport monitor rate-limit 1G

no switchport monitor rate-limit [1G]

Syntax Description	1G (Optional) Specifies that the rate limit is 1 GB.
---------------------------	---

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

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

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

Usage Guidelines	<p>This command is applicable to the following Cisco Nexus 5000 Series switches:</p> <ul style="list-style-type: none"> • Cisco Nexus 5010 Series • Cisco Nexus 5020 Series <p>This command does not require a license.</p>
-------------------------	---

Examples	<p>This example shows how to limit the bandwidth on Ethernet interface 1/2 to 1 GB:</p> <pre>switch(config)# interface ethernet 1/2 switch(config-if)# switchport monitor rate-limit 1G switch(config-if)#</pre>
-----------------	--

Related Commands	Command	Description
	show interface switchport	Displays information on all interfaces configured as switch ports.
switchport private-vlan association trunk	Associates the isolated trunk port with the primary and secondary VLANs of a private VLAN.	

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

switch-profile

To create or configure a switch profile, use the **switch-profile** command. To delete a switch profile, use the **no** form of this command.

switch-profile *sw-profile-name*

no switch-profile *sw-profile-name* {**all-config** | **local-config** | **profile-only**}

Syntax Description

<i>sw-profile-name</i>	Name of the switch profile. The name is case sensitive, can be a maximum of 64 alphanumeric characters and can include an underscore and hyphen. The name cannot contain spaces or special characters.
all-config	Specifies that the switch profile be deleted with all local and peer configurations.
local-config	Specifies that the switch profile and all local configurations be deleted.
profile-only	Specifies that the switch profile only is to be deleted and no other configurations.

Command Default

None

Command Modes

Configuration synchronization mode

Command History

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

Usage Guidelines

Use this command to create a switch profile on each of the peer switches. You must use the same profile name on both the switches in the Cisco Fabric Services (CFS) peer configuration.



Note

In this release of Cisco NX-OS, only a pair of switches can be configured as a peer.

You can configure only one active switch profile on each peer switch. If you create or configure a second switch profile, you see the following error message:

```
Error: Another switch profile already exists. Cannot configure more than one switch-profile.
```

The configuration that is made locally on the switch is synchronized and made available on the peer switch only after the connectivity is established between the peer switches and the configuration is verified and committed on the local switch.

You can configure a switch profile to include the interface configuration, quality of service (QoS), and virtual port channel (vPC) commands. FCoE commands are not supported on a switch profile.

Send comments to nexus5k-docfeedback@cisco.com

When you delete a switch profile, you can choose to delete the local switch profile with the local configurations on the switch, delete the switch profile with the local configurations and configuration information in the peer, or delete the switch profile only while saving all other configuration information. The peer becomes unreachable.

Examples

This example shows how to create a switch profile named s5010 on switch 1 of the peer:

Peer A

```
switch# configure terminal
switch(config)# cfs ipv4 distribute
switch(config)# exit
switch# config sync
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-sync)# switch-profile s5010
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)#
```

This example shows how to create a switch profile named s5010 on switch 2 of the peer:

Peer B

```
switch# configure terminal
switch(config)# cfs ipv4 distribute
switch(config)# exit
switch# config sync
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-sync)# switch-profile s5010
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)#
```

This example shows how to delete a switch profile named s5010 and its local configuration on switch 1 of the peer:

Peer A

```
switch# config sync
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-sync)# no switch-profile s5010 local-config
switch(config-sync)#
```

Related Commands

Command	Description
config sync	Enters configuration synchronization mode.
show switch-profile	Displays the switch profile created on the switch and its configuration revision.
sync-peers destination	Configures the peer switch for configuration synchronization.

Send comments to nexus5k-docfeedback@cisco.com

system ethernet dom polling

To enable transceiver digital optical monitoring periodic polling, use the **system ethernet dom polling** command. To disable transceiver digital optical monitoring periodic polling, use the **no** form of this command.

system ethernet dom polling

no system ethernet dom polling

Syntax Description This command has no arguments or keywords

Command Default Disabled

Command Modes Configuration mode

Command History	Release	Modification
	5.2(1)N1(5)	This command was introduced.

Usage Guidelines Use this command to enable transceiver digital optical monitoring periodic polling.

Examples This example shows how to enable transceiver digital optical monitoring periodic polling:

```
switch# configure terminal
switch(config)# system ethernet dom polling
```

Related Commands	Command	Description
	show system ethernet dom polling status	Displays the status of transceiver digital optical monitoring periodic polling.

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com



Show Commands

This chapter describes the system management **show** commands.

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

show diagnostic bootup level

To display the current bootup diagnostic level on the switch, use the **show diagnostic bootup level** command.

show diagnostic bootup level

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

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

Examples This example shows how to display the current bootup diagnostic level:

```
switch# show diagnostic bootup level

Current bootup diagnostic level: complete

switch#
```

Related Commands	Command	Description
	diagnostic bootup level	Configures the bootup diagnostic level for a faster module bootup time.
	show diagnostic result	Displays the results of the diagnostics tests.

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

show diagnostic result

To display the results of the diagnostic tests, use the **show diagnostic result** command.

show diagnostic result module {*module-no* | **all**}

Syntax Description	module	Specifies the module for which diagnostic results are displayed.
	<i>module-no</i>	Module number. Valid values are 1 to 3.
	all	Displays the diagnostic results for all modules.

Command Default None

Command Modes EXEC mode

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

Examples This example shows how to display the diagnostic results for a specific module:

```
switch# show diagnostic result module 1

Current bootup diagnostic level: complete

Module 1: 48X10GE/Supervisor SerialNo : JAF1339ANGH

Overall Diagnostic Result for Module 1 : PASS
Diagnostic level at card bootup: complete

Test results: (. = Pass, F = Fail, I = Incomplete,
              U = Untested, A = Abort)

    1) TestUSBFlash -----> .
    2) TestSPROM -----> .
    3) TestPCIE -----> .
    4) TestLED -----> .
    5) TestOBFL -----> .
    6) TestNVRAM -----> .
    7) TestPowerSupply -----> F
    8) TestTemperatureSensor -----> .
    9) TestFan -----> .
   10) TestVoltage -----> .
   11) TestGPIO -----> .
   12) TestInbandPort -----> .
   13) TestManagementPort -----> .
   14) TestMemory -----> .
   15) TestFabricEngine :

Eth   1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Port -----
      .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
```

Send comments to nexus5k-docfeedback@cisco.com

```

Eth  25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
Port -----
. . . . .

16) TestFabricPort :

Eth   1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Port -----
. . . . .

Eth  25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
Port -----
. . . . .

17) TestForwardingEngine :

Eth   1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Port -----
. . . . .

Eth  25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
Port -----
. . . . .

18) TestForwardingEnginePort :

Eth   1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Port -----
. . . . .

Eth  25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
Port -----
. . . . .

19) TestFrontPort :

Eth   1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Port -----
. . . . .

Eth  25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
Port -----
. . . . .

switch#

```

Related Commands

Command	Description
diagnostic bootup level	Configures the bootup diagnostic level for a faster module bootup time.
show diagnostic bootup level	Displays the bootup diagnostics level.

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

show hosts

To display the Domain Name Server (DNS) name servers and domain names, use the **show hosts** command.

show hosts

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

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

Examples This example shows how to display the IP addresses of the DNS servers that are used to resolve host names:

```
switch# show hosts
DNS lookup enabled
Default domain for vrf:default is mysite.com
Name/address lookup uses domain service
Name servers are 255.255.255.255
```

Vrf	Use-vrf	Token	Config
default	management	domain	mysite.com
default	management	add. domain(s)	mysite2.com

```
Host
switch#
```

Related Commands	Command	Description
	ip domain-list	Defines a list of domains.
	ip domain lookup	Enables DNS-based host name-to-address translation.
	ip domain-name	Configures a name server.

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

show ip dns source-interface

To display the source interfaces configured for Domain Name Server (DNS) domain lookup, use the **show ip dns source-interface** command.

```
show ip dns source-interface [vrf {vrf-name | all | default | management}]
```

Syntax Description		
vrf	(Optional)	Displays information about the virtual routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional)	VRF name. The name is case sensitive and can be a maximum of 32 characters.
all	(Optional)	Displays all VRF instances.
default	(Optional)	Displays the default VRF information.
management	(Optional)	Displays the management VRF information.

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 source interfaces configured for DNS domain lookup:

```
switch# show ip dns source-interface
VRF Name      Interface
default       Ethernet1/5
switch#
```

Related Commands	Command	Description
	ip domain-lookup	Enables the DNS lookup feature.
	ip dns source-interface	Configures interfaces for DNS domain lookup.

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

show logging console

To display the console logging configuration, use the **show logging console** command.

show logging console

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 console logging configuration:

```
switch# show logging console
```

Related Commands	Command	Description
	logging console	Configures logging to the console.

Send comments to nexus5k-docfeedback@cisco.com

show logging info

To display the logging configuration, use the **show logging info** command.

show logging info

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 logging configuration:

```
switch# show logging info
```

Related Commands	Command	Description
	logging level	Enables logging messages from a defined facility.

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

show logging last

To display the last number of lines of the logfile, use the **show logging last** command.

show logging last *number*

Syntax Description	<i>number</i>	Enters the number of lines to display from 1 to 9999.
---------------------------	---------------	---

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 last 42 lines of the log file:
-----------------	--

```
switch# show logging last 42
```

Related Commands	Command	Description
	logging level	Enables logging messages from a defined facility.

Send comments to nexus5k-docfeedback@cisco.com

show logging level

To display the facility logging severity level configuration, use the **show logging level** command.

```
show logging level [facility]
```

Syntax Description	<i>facility</i>	(Optional) Logging facility. The facilities are listed in Table 1-1 of Appendix 1, "System Message Logging Facilities."
---------------------------	-----------------	---

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

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

Command History	Release	Modification
	4.0(0)N1(1a)	This command was introduced.
	5.0(3)N1(1)	Support for multicast and unicast routing features was added.
	5.0(3)N2(1)	Support for Flex Links and Fibre Channel over Ethernet (FCoE) N-Port Virtualizer (NPV) was added.

Examples

This example shows how to display the EtherChannel logging severity level configuration:

```
switch# show logging level port-channel
```

This example shows how to display the Flex Links logging severity level configuration:

```
switch# show logging level flexlink
Facility          Default Severity      Current Session Severity
-----          -
Flexlink          2                      5

0 (emergencies)   1 (alerts)            2 (critical)
3 (errors)        4 (warnings)          5 (notifications)
6 (information)   7 (debugging)
```

```
switch#
```

This example shows how to display the FCoE NPV logging severity level configuration:

```
switch# show logging level fcoe_mgr
Facility          Default Severity      Current Session Severity
-----          -
fcoe_mgr          2                      3

0 (emergencies)   1 (alerts)            2 (critical)
3 (errors)        4 (warnings)          5 (notifications)
6 (information)   7 (debugging)
```

```
switch#
```


Send comments to nexus5k-docfeedback@cisco.com

Related Commands

Command	Description
logging level	Configures the facility logging level.

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

show logging logfile

To display the messages in the log file that were timestamped within the span entered, use the **show logging logfile** command.

show logging logfile [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*]

Syntax Description

start-time <i>yyyy mmm dd hh:mm:ss</i>	(Optional) Specifies a start time in the format <i>yyyy mmm dd hh:mm:ss</i> . Use three characters for the month (<i>mmm</i>) field, digits for the year (<i>yyyy</i>) and day (<i>dd</i>) fields, and digits separated by colons for the time (<i>hh:mm:ss</i>) field.
end-time <i>yyyy mmm dd hh:mm:ss</i>	(Optional) Specifies an end time in the format <i>yyyy mmm dd hh:mm:ss</i> . Use three characters for the month (<i>mmm</i>) field, digits for the year (<i>yyyy</i>) and day (<i>dd</i>) fields, and digits separated by colons for the time (<i>hh:mm:ss</i>) field.

Command Default

None

Command Modes

EXEC mode

Command History

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

Usage Guidelines

If you do not enter an end time, the current time is used.

Examples

This example shows how to display the messages in the log file that were timestamped within the span shown:

```
switch# show logging logfile start-time 2008 mar 11 12:10:00
```

Related Commands

Command	Description
logging logfile	Configures logging to a log file.

Send comments to nexus5k-docfeedback@cisco.com

show logging module

To display the module logging configuration, use the **show logging module** command.

show logging module

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 module logging configuration:

```
switch# show logging module
```

Related Commands	Command	Description
	logging module	Configures module logging.

Send comments to nexus5k-docfeedback@cisco.com

show logging monitor

To display the monitor logging configuration, use the **show logging monitor** command.

show logging monitor

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 monitor logging configuration:

```
switch# show logging monitor
```

Related Commands	Command	Description
	logging monitor	Configures logging on the monitor.

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

show logging nvram

To display the messages in the nonvolatile random access memory (NVRAM) log, use the **show logging nvram** command.

```
show logging nvram [last number-lines]
```

Syntax Description	last <i>number-lines</i> (Optional) Specifies the number of lines to display. The number of lines is from 1 to 100.				
Command Default	None				
Command Modes	EXEC mode				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>4.0(0)N1(1a)</td><td>This command was introduced.</td></tr></tbody></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 the last 20 messages in the NVRAM log: <pre>switch# show logging nvram last 20</pre>				
Related Commands	<table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>logging level</td><td>Enables logging messages from a defined facility.</td></tr></tbody></table>	Command	Description	logging level	Enables logging messages from a defined facility.
Command	Description				
logging level	Enables logging messages from a defined facility.				

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

show logging onboard

To display the onboard logging information based on the error type, use the **show logging onboard** command.

```
show logging onboard { boot-uptime | device-version | endtime | environmental-history |
exception-log | kernel-trace | obfl-history | obfl-logs | stack-trace | starttime | status } [> file
| | type]
```

Syntax	Description
boot-uptime	Displays the onboard failure logging (OBFL) boot and uptime information.
device-version	Displays the OBFL device version information.
endtime	Displays the OBFL logs until the specified end time in the following format: <i>mm/dd/yy-HH:MM:SS</i>
environmental-history	Displays the OBFL environmental history.
exception-log	Displays the OBFL exception log.
kernel-trace	Displays the OBFL kernel trace information.
obfl-history	Displays the OBFL history information.
obfl-logs	Displays the OBFL technical support log information.
stack-trace	Displays the OBFL kernel stack trace information.
starttime	Displays the OBFL logs from the specified start time in the following format: <i>mm/dd/yy-HH:MM:SS</i>
status	Displays the OBFL status enable or disable.
> file	(Optional) Redirects the output to a file. See the “Usage Guidelines” section for additional information.
 type	(Optional) Filters the output. See the “Usage Guidelines” section for additional information.

Command Default None

Command Modes EXEC mode

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

Usage Guidelines The date and time arguments for the **starttime** and **endtime** keywords are entered as the date month/day/year (*mm/dd/yy*), followed by a hyphen, and the time in 24-hour format in hours:minutes:seconds (*HH:MM:SS*). For example:

- **starttime** 03/17/08-15:01:57
- **endtime** 03/18/08-15:04:57

The valid values for *file* are as follows:

Send comments to nexus5k-docfeedback@cisco.com

- **bootflash:**
- **ftp:**
- **scp:**
- **sftp:**
- **tftp:**
- **volatile:**

The valid values for *type* are as follows:

- **begin [-i] [-x] [word]**—Begin with the line that matches the text.
 - **-i**—Ignores the case difference when comparing the strings.
 - **-x**—Prints only the lines where the match is a whole line.
 - *word*—Specifies for the expression.
- **count [> file || type]**—Counts number of lines.
- **egrep | grep print-match**—Egrep or Grep. Egrep searches for lines of text that match more sophisticated regular expression syntax than grep. Grep searches for lines of text that match one or many regular expressions, and outputs only the matching lines.
 - **-A num**—Prints the specifies number of lines of context after every matching line. Range: 1 to 999.
 - **-B num**—Prints the specifies number of lines of context before every matching line. Range: 1 to 999.
 - **-c**—Prints a total count of matching lines only.
 - **-i**—Ignores the case difference when comparing the strings.
 - **-n**—Prints each match preceded by its line number.
 - **-v**—Prints only the lines that contain no matches for the *word* argument.
 - **-w**—Prints only lines where the match is a complete word.
 - **-x**—Prints only the lines where the match is a whole line.
 - *word*—Specifies for the expression.
- **exclude [-i] [-x] [word]**—Excludes the lines that match.
 - **-i**—Ignores the case difference when comparing the strings.
 - **-x**—Prints only the lines where the match is a whole line.
 - *word*—Specifies for the expression.
- **head [-n num]**—Stream Editor. The optional **-n num** keyword and argument allow you to specify the number of lines to print. Range: 0 to 2147483647.
- **include [-i] [-x] [word]**—Include the lines that match.
 - **-i**—Ignores the case difference when comparing the strings.
 - **-x**—Prints only the lines where the match is a whole line.
 - *word*—Specifies for the expression.
- **last [num]**—Displays the last lines to print. The optional *num* specifies the number of lines to print. Range: 0 to 9999.
- **less [-E | -d]**—Quits at the end of the file.

Send comments to nexus5k-docfeedback@cisco.com

- **-E**—(Optional) Quits at the end of the file.
- **-d**—(Optional) Specifies a dumb terminal.
- **no-more**—Turns-off pagination for command output.
- **sed command**—Stream Editor
- **wc**—Counts words, lines, and characters.
 - **-c**—(Optional) Specifies the output character count.
 - **-l**—(Optional) Specifies the output line count.
 - **-w**—(Optional) Specifies the output word count.
 - **>**—Redirects it to a file.
 - **|**—Pipes command output to filter.

Use this command to view OBFL data from the system hardware. The OBFL feature is enabled by default and records operating temperatures, hardware uptime, interrupts, and other important events and messages that can assist with diagnosing problems with hardware cards or modules installed in a Cisco router or switch. Data is logged to files stored in nonvolatile memory. When the onboard hardware is started up, a first record is made for each area monitored and becomes a base value for subsequent records.

The OBFL feature provides a circular updating scheme for collecting continuous records and archiving older (historical) records, ensuring accurate data about the system. Data is recorded in one of two formats: continuous information that displays a snapshot of measurements and samples in a continuous file, and summary information that provides details about the data being collected. The message “No historical data to display” is seen when historical data is not available.

Examples

This example shows how to display the OBFL boot and uptime information:

```
switch# show logging onboard boot-uptime
Sun Nov  9 06:11:59 2008:  Boot Record
-----
Boot Time.....:  Sun Nov  9 06:11:58 2008
Slot Number.....:  1
Serial Number.....:  FLC12280050
Bios Version.....:  v1.2.0(06/19/08)
Firmware Version...:  4.0(1a)N1(1) [build 4.0(1a)N1(1)]
```

[Table 1](#) describes the significant fields shown in the display.

Table 1 *show logging onboard boot-uptime Command Output*

Field	Description
Boot Time	Time boot occurred.
Slot Number	Slot number.
Serial Number	Serial number of the module.
Bios Version	Primary binary input and output system (BIOS) version.
Firmware Version	Firmware version.

Send comments to nexus5k-docfeedback@cisco.com

This example shows how to display the OBFL logging device information:

```
switch# show logging onboard device-version
-----
OBFL Data for
  Module: 1
-----

Device Version Record
-----
Timestamp                Device Name      Instance Hardware Software
                        Num   Version   Version
-----
Sun Nov  3 07:07:00 2008   GATOS           2         2         0
Sun Nov  3 07:07:00 2008   GATOS           3         2         0
Sun Nov  3 07:07:00 2008   GATOS           4         2         0
Sun Nov  3 07:07:00 2008   GATOS           5         2         0
Sun Nov  3 07:07:00 2008   GATOS           6         2         0
Sun Nov  3 07:07:00 2008   GATOS           7         2         0
Sun Nov  3 07:07:00 2008   GATOS           8         2         0
Sun Nov  3 07:07:00 2008   GATOS           9         2         0
Sun Nov  3 07:07:00 2008   GATOS          10         2         0
Sun Nov  3 07:07:00 2008   GATOS          11         2         0
Sun Nov  3 07:07:00 2008   GATOS          12         2         0
Sun Nov  3 07:07:00 2008   GATOS          13         2         0
Mon Nov  4 00:15:08 2008   ALTOS           0         2         0
Mon Nov  4 00:15:08 2008   GATOS           0         2         0
Mon Nov  4 00:15:08 2008   GATOS           1         2         0
Mon Nov  4 00:15:08 2008   GATOS           2         2         0
```

[Table 2](#) describes the significant fields shown in the display.

Table 2 *show logging onboard device-version Command Output*

Field	Description
Timestamp	Day, date, and time.
Device Name	Device name.
Instance Num	Number of instances.
Hardware Version	Hardware device version.
Software Version	Software device version.

This example shows how to display the OBFL history information:

```
switch# show logging onboard obfl-history
```

The **show logging onboard obfl-history** command displays the following information:

- Timestamp when OBFL is manually disabled.
- Timestamp when OBFL is manually enabled.
- Timestamp when OBFL data is manually cleared.

This example shows how to display the OBFL kernel stack trace information:

```
switch# show logging onboard stack-trace
```

The **show logging onboard stack-trace** command displays the following information:

- Time in seconds

■ show logging onboard

Send comments to nexus5k-docfeedback@cisco.com

- Time in microseconds
- Error description string
- Current process name and identification
- Kernel jiffies
- Stack trace

Related Commands

Command	Description
clear logging onboard	Clears the OBFL entries in the persistent log.
hw-module logging onboard	Enables or disabled OBFL entries based on the error type.

Send comments to nexus5k-docfeedback@cisco.com

show logging pending

To display the pending changes to the syslog server configuration, use the **show logging pending** command.

show logging pending

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

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

Examples This example shows how to display the pending changes to the syslog server configuration:

```
switch# show logging pending
switch#
```

Related Commands	Command	Description
	logging abort	Cancels the pending changes to the syslog server configuration.

Send comments to nexus5k-docfeedback@cisco.com

show logging pending-diff

To display the differences from the current syslog server configuration to the pending changes of the syslog server configuration, use the **show logging pending-diff** command.

show logging pending-diff

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

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

Examples This example shows how to display the pending differences of the syslog server configuration:

```
switch# show logging pending-diff
switch#
```

Related Commands	Command	Description
	logging abort	Cancels the pending changes to the syslog server configuration.

Send comments to nexus5k-docfeedback@cisco.com

show logging session status

To display the logging session status, use the **show logging session status** command.

show logging session status

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 logging session status:

```
switch# show logging session status
```

Related Commands	Command	Description
	logging level	Enables logging messages from a defined facility.

Send comments to nexus5k-docfeedback@cisco.com

show logging server

To display the syslog server configuration, use the **show logging server** command.

show logging 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 syslog server configuration:

```
switch# show logging server
```

Related Commands	Command	Description
	logging server	Configures a remote syslog server.

Send comments to nexus5k-docfeedback@cisco.com

show logging status

To display the logging status, use the **show logging status** command.

show logging status

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

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

Examples This example shows how to display the logging status:

```
switch# show logging status
Fabric Distribute      : Enabled
Session State         : IDLE
switch#
```

Command	Description
logging distribute	Enables the distribution of the syslog server configuration to network switches using the Cisco Fabric Services (CFS) infrastructure.

Send comments to nexus5k-docfeedback@cisco.com

show logging timestamp

To display the logging time-stamp configuration, use the **show logging timestamp** command.

show logging timestamp

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 logging time-stamp configuration:

```
switch# show logging timestamp
```

Related Commands	Command	Description
	logging timestamp	Configures the logging time stamp granularity.

Send comments to nexus5k-docfeedback@cisco.com

show ntp authentication-status

To display the status of the Network Time Protocol (NTP) authentication, use the **show ntp authentication-status** command.

show ntp authentication-status

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 authentication status for NTP:

```
switch(config)# show ntp authentication-status
```

Related Commands	Command	Description
	[no] ntp authenticate	Displays information about NTP peers.

Send comments to nexus5k-docfeedback@cisco.com

show ntp peer-status

To display the status of the Network Time Protocol (NTP) peers, use the **show ntp peer-status** command.

show ntp peer-status

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 peer status for NTP:

```
switch(config)# show ntp peer-status
```

Related Commands	Command	Description
	show ntp peers	Displays information about NTP peers.

Send comments to nexus5k-docfeedback@cisco.com

show ntp peers

To display information about Network Time Protocol (NTP) peers, use the **show ntp peers** command.

```
show ntp peers
```

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 information about NTP peers:

```
switch(config)# show ntp peers
```

Related Commands	Command	Description
	show ntp peer-status	Displays status information about NTP peers.

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

show ntp statistics

To display Network Time Protocol (NTP) statistics, use the **show ntp statistics** command.

```
show ntp statistics {io | local | memory | peer} {ipaddr address | name name1 [..nameN]}
```

Syntax	Description
io	Displays the input-output statistics.
local	Displays the counters maintained by the local NTP.
memory	Displays the statistics counters related to the memory code.
peer	Displays the per-peer statistics counter of a peer.
ipaddr <i>address</i>	Displays statistics for the peer with the configured IPv4 or IPv6 address. The IPv4 address format is dotted decimal, x.x.x.x. The IPv6 address format is hexadecimal A:B::C:D.
name <i>name1</i>	Displays statistics for a named peer.
<i>..nameN</i>	(Optional) Displays statistics for one or more named peers.

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 statistics for NTP:

```
switch(config)# show ntp statistics local
```

Related Commands	Command	Description
	clear ntp statistics	Clears NTP statistics

Send comments to nexus5k-docfeedback@cisco.com

show ntp timestamp-status

To display the Network Time Protocol (NTP) time-stamp information, use the **show ntp timestamp-status** command.

show ntp timestamp-status

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 NTP time-stamp status:

```
switch(config)# show ntp timestamp-status
```

Related Commands	Command	Description
	clear ntp statistics	Clears NTP statistics
	ntp	Configures NTP peers and servers on the switch.

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

show ptp brief

To display the PTP information, use the **show ptp brief** command.

show ptp brief

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration mode

Command History	Release	Modification
	5.2(1)N1(1)	This command was introduced.

Examples This example shows how to display the PTP status:

```
switch(config)# show ptp brief
```

Related Commands	Command	Description
	show ptp clock	Displays the properties of the local clock.
	show ptp clocks foreign-masters-record	Displays the state of foreign masters known to the PTP process.
	show ptp corrections	Displays the last few PTP corrections.
	show ptp parent	Displays the properties of the PTP parent and grandmaster clock.
	show ptp port interface	Displays the status of the PTP port.
	show ptp time-property	Displays the PTP clock time properties.

Send comments to nexus5k-docfeedback@cisco.com

show ptp clock

To display the properties of the local PTP clock including clock identity, use the **show ptp clock** command.

show ptp clock

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration mode

Command History	Release	Modification
	5.2(1)N1(1)	This command was introduced.

Examples This example shows how to display the properties of the local clock:

```
switch(config)# show ptp clock
```

Related Commands	Command	Description
	show ptp brief	Displays the PTP status.
	show ptp clocks foreign-masters-record	Displays the state of foreign masters known to the PTP process.
	show ptp corrections	Displays the last few PTP corrections.
	show ptp parent	Displays the properties of the PTP parent and grandmaster clock.
	show ptp port interface	Displays the status of the PTP port.
	show ptp time-property	Displays the PTP clock time properties.

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

show ptp clocks foreign-masters-record

To display the state of the foreign masters known to the PTP process, use the **show ptp clocks foreign-masters-record** command.

```
show ptp clocks foreign-masters-record [ethernet slot/port]
```

Syntax Description

ethernet	Specifies an Ethernet interface.
<i>slot/port</i>	The slot ID and port ID for the Ethernet interface.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

For each foreign master, the output displays the clock identity, basic clock properties, and whether the clock is being used as a grandmaster.

Examples

This example shows how to display the foreign masters known to the PTP process:

```
switch(config)# show ptp foreign-masters-record
```

Related Commands

Command	Description
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.
show ptp corrections	Displays the last few PTP corrections.
show ptp port interface	Displays the status of the PTP port.
show ptp parent	Displays the properties of the PTP parent and grandmaster clock.
show ptp time-property	Displays the PTP clock time properties.

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

show ptp corrections

To display the last few PTP corrections, use the **show ptp corrections** command.

show ptp corrections

Syntax Description There are no arguments or keywords for this command.

Command Default None

Command History	Release	Modification
	5.2(1)N1(1)	This command was introduced.

Examples This example shows how to display the most recent PTP corrections on the switch:

```
switch(config)# show ptp corrections
```

Related Commands	Command	Description
	show ptp brief	Displays the PTP status.
	show ptp clock	Displays the properties of the local clock.
	show ptp clocks foreign-masters-record	Displays the state of foreign masters known to the PTP process.
	show ptp port interface	Displays the status of the PTP port.
	show ptp parent	Displays the properties of the PTP parent and grandmaster clock.
	show ptp time-property	Displays the PTP clock time properties.

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

show ptp parent

To display the properties of the PTP parent and grandmaster clock, use the **show ptp parent** command.

show ptp parent

Syntax Description There are no arguments or keywords for this command.

Command Default None

Command History	Release	Modification
	5.2(1)N1(1)	This command was introduced.

Examples This example shows how to display the properties of the PTP parent and grandmaster clock:

```
switch(config)# show ptp parent
```

Related Commands	Command	Description
	show ptp brief	Displays the PTP status.
	show ptp clock	Displays the properties of the local clock.
	show ptp clocks foreign-masters-record	Displays the state of foreign masters known to the PTP process.
	show ptp corrections	Displays the last few PTP corrections.
	show ptp port interface	Displays the status of the PTP port.
	show ptp time-property	Displays the PTP clock time properties.

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

show ptp port interface

To display the status of the PTP port, use the **show ptp port interface ethernet** command.

```
show ptp port interface [ethernet slot/port]
```

Syntax Description	Parameter	Description
	ethernet	Specifies an Ethernet interface.
	<i>slot/port</i>	The slot ID and port ID for the Ethernet interface.

Command Default None

Command Modes Global configuration mode

Command History	Release	Modification
	5.2(1)N1(1)	This command was introduced.

Examples This example shows how to display the status of the PTP port on the switch:

```
switch(config)# show ptp port interface ethernet 5/1
```

Related Commands	Command	Description
	show ptp brief	Displays the PTP status.
	show ptp clock	Displays the properties of the local clock.
	show ptp clocks foreign-masters-record	Displays the state of foreign masters known to the PTP process.
	show ptp corrections	Displays the last few PTP corrections.
	show ptp port interface	Displays the status of the PTP port.
	show ptp parent	Displays the properties of the PTP parent and grandmaster clock.
	show ptp time-property	Displays the PTP clock time properties.

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

show ptp time-property

To display the PTP clock time properties, use the **show ptp time-property** command.

```
show ptp time-property
```

Syntax Description There are no arguments or keywords for this command.

Command Default None

Command History	Release	Modification
	5.2(1)N1(1)	This command was introduced.

Examples This example shows how to display the PTP clock time properties:

```
switch(config)# show ptp time-property
```

Related Commands	Command	Description
	show ptp brief	Displays the PTP status.
	show ptp clock	Displays the properties of the local clock.
	show ptp clocks foreign-masters-recor d	Displays the state of foreign masters known to the PTP process.
	show ptp corrections	Displays the last few PTP corrections.
	show ptp parent	Displays the properties of the PTP parent and grandmaster clock.
	show ptp port interface	Displays the status of the PTP port.

Send comments to nexus5k-docfeedback@cisco.com

show snmp community

To display the Simple Network Management Protocol (SNMP) community strings configured on the switch, use the **show snmp community** command.

show snmp community

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

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

Examples This example shows how to display the SNMP community strings:

```
switch# show snmp community
Community          Group / Access      context      acl_filter
-----          -
public            network-admin
switch#
```

Related Commands	Command	Description
	snmp-server community	Configures the community access string to permit access to the SNMP protocol.

Send comments to nexus5k-docfeedback@cisco.com

show snmp context

To display the Simple Network Management Protocol (SNMP) contexts configured on the switch, use the **show snmp context** command.

show snmp context

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

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

Examples This example shows how to display the SNMP contexts:

```
switch# show snmp context
```

Related Commands	Command	Description
	snmp-server context	Configures an SNMP context.

Send comments to nexus5k-docfeedback@cisco.com

show snmp engineID

To display the identification of the local Simple Network Management Protocol (SNMP) engine, use the **show snmp engineID** command.

show snmp engineID

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

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

Usage Guidelines An SNMP engine is a copy of SNMP that can reside on a local or remote device. SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine.

Examples This example shows how to display the SNMP engine ID:

```
switch# show snmp engineID
Local SNMP engineID: [Hex] 8000000903000DECB230C0
                    [Dec] 128:000:000:009:003:000:013:236:178:048:192
switch#
```

Related Commands	Command	Description
	show running-config snmp	Displays the running configuration information about SNMP.

Send comments to nexus5k-docfeedback@cisco.com

show snmp group

To display the names of the Simple Network Management Protocol (SNMP) groups configured on the switch, use the **show snmp group** command.

show snmp group

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

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

Examples This example shows how to display the SNMP groups:

```
switch# show snmp group
```

```
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
```

```
-----
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
```


Send comments to nexus5k-docfeedback@cisco.com

```
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)
```

```
-----
```

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 *
1	permit	read		

```
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		

```
switch#
```

Related Commands

Command	Description
show running-config snmp	Displays the running configuration information about SNMP.

Send comments to nexus5k-docfeedback@cisco.com

show snmp host

To display the Simple Network Management Protocol (SNMP) host information, use the **show snmp host** command.

show snmp host

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

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

Examples This example shows how to display the SNMP host:

```
switch# show snmp host
```

Related Commands	Command	Description
	snmp-server host	Configures an SNMP host.

Send comments to nexus5k-docfeedback@cisco.com

show snmp sessions

To display the current Simple Network Management Protocol (SNMP) sessions, use the **show snmp sessions** command.

show snmp sessions

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

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

Examples This example shows how to display the SNMP sessions:

```
switch# show snmp sessions
```

Related Commands	Command	Description
	show running-config snmp	Displays the running configuration information about SNMP.

Send comments to nexus5k-docfeedback@cisco.com

show snmp trap

To display the Simple Network Management Protocol (SNMP) link trap generation information, use the **show snmp trap** command.

show snmp trap

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

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

Examples This example shows how to display the SNMP traps:

```
switch# show snmp trap
```

```
-----
Trap type           Description           Enabled
-----
entity              : entity_mib_change   Yes
entity              : entity_module_status_change   Yes
entity              : entity_power_status_change   Yes
entity              : entity_module_inserted   Yes
entity              : entity_module_removed   Yes
entity              : entity_unrecognised_module   Yes
entity              : entity_fan_status_change   Yes
link                : linkDown            Yes
link                : linkUp              Yes
link                : IETF-extended-linkDown   Yes
link                : IETF-extended-linkUp    Yes
link                : cisco-extended-linkDown  Yes
link                : cisco-extended-linkUp    Yes
callhome            : event-notify        No
callhome            : smtp-send-fail       No
cfs                 : state-change-notif   No
cfs                 : merge-failure        No
rf                  : redundancy_framework  Yes
aaa                 : server-state-change   No
license             : notify-license-expiry  Yes
license             : notify-no-license-for-feature  Yes
license             : notify-licensefile-missing  Yes
license             : notify-license-expiry-warning  Yes
zone                : unsupp-mem          No
upgrade             : UpgradeOpNotifyOnCompletion  Yes
upgrade             : UpgradeJobStatusNotify  Yes
feature-control     : FeatureOpStatusChange  No
sysmgr              : cseFailSwCoreNotifyExtended  No
rmon                : risingAlarm          No
-----
```

Send comments to nexus5k-docfeedback@cisco.com

```

rmon          : fallingAlarm          No
rmon          : hcRisingAlarm         No
rmon          : hcFallingAlarm        No
config        : ccmCLIRunningConfigChanged No
snmp          : authentication        No
bridge        : topologychange        No
bridge        : newroot               No
stp           : inconsistency          No
stp           : loop-inconsistency     No
stp           : root-inconsistency     No
switch#

```

Related Commands

Command	Description
snmp trap link-status	Enables SNMP link trap generation.

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

show snmp user

To display information on each Simple Network Management Protocol (SNMP) user, use the **show snmp user** command.

show snmp user

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	4.1(3)N2(1)	This command was introduced.

Examples This example shows how to display the SNMP users configured on the switch:

```
switch# show snmp user
```

```
SNMP USERS
```

User	Auth	Priv(enforce)	Groups
admin	md5	des(no)	network-admin

```
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
```

User	Auth	Priv

```
switch#
```

This example shows how to display information about a specific SNMP user:

```
switch# show snmp user admin
switch#
```

Related Commands	Command	Description
	snmp-server user	Configures a new user to an SNMP group.

Send comments to nexus5k-docfeedback@cisco.com

show system ethernet dom polling status

To display the status of transceiver digital optical monitoring periodic polling, use the **show system ethernet dom polling status** command.

show system ethernet dom polling status

Syntax Description This command has no arguments or keywords

Command Default None

Command Modes EXEC mode

Release	Modification
5.2(1)N1(5)	This command was introduced.

Usage Guidelines Use this command to display the status of transceiver digital optical monitoring periodic polling.

Examples This example shows how to display the status of transceiver digital optical monitoring periodic polling:

```
switch# show system ethernet dom polling status
Ethernet DOM Polling Status: enabled
```

Command	Description
system ethernet dom polling	Enables transceiver digital optical monitoring periodic polling.

■ show system ethernet dom polling status

Send comments to nexus5k-docfeedback@cisco.com

Send comments to nexus5k-docfeedback@cisco.com



V Commands

This chapter describes the system management commands available that begin with V.

Send comments to nexus5k-docfeedback@cisco.com

verify (session)

To verify the current configuration session, use the **verify** command.

verify

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Session configuration mode

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

Examples This example shows how to verify a session:

```
switch(config-s)# verify
Failed to start Verification: Session Database already locked, Verify/Commit in
Progress.
switch(config-s)#
```

Related Commands	Command	Description
	commit	Commits a session.
	configure session	Creates a configuration session.
	show configuration session	Displays the contents of the session.



APPENDIX 1

System Message Logging Facilities

This appendix contains the system message logging information. [Table 1-1](#) lists the facilities that you can use in system message logging configuration.

Table 1-1 System Message Logging Facilities

Facility	Description
aaa	Sets level for aaa syslog messages.
aclmgr	Sets level for aclmgr syslog messages.
adjmgr	Sets syslog filter level for Adjacency Manager.
afm	Sets level for afm syslog messages.
all	Sets level for all facilities.
altos	Altos syslog level.
arp	Sets syslog filter level for ARP.
ascii-cfg	Sets the logging level for ascii-cfg.
auth	Sets level for Authorization System.
authpriv	Sets level for Authorization (Private) system.
backup	Sets level for switchport backup syslog messages.
bootvar	Sets level for bootvar.
callhome	Callhome syslog level.
capability	Sets syslog level for mig utils daemon.
cdp	Sets logging level for CDP.
cert-enroll	Cert-enroll syslog level.
cfs	Sets logging level for CFS.
clis	Sets syslog filter level for CLIS.
core	Core daemon syslog level.
cron	Sets level for Cron/at facility.
daemon	Sets level for System daemons.
dcbx	Sets level for dcx syslog messages.
device-alias	Sets syslog level for Device Alias Distribution Service.
dhcp_snoop	Sets the level for DHCP snooping syslog messages.

Send comments to nexus5k-docfeedback@cisco.com

Table 1-1 System Message Logging Facilities (continued)

Facility	Description
dstats	Delta statistics syslog level.
epp	Sets level for EPP syslog messages.
ethpc	Sets level for ethpc syslog messages.
ethpm	Sets level for Ethernet Port Manager (ethpm) syslog messages.
evmc	Sets level for evmc syslog messages.
fabric_start_cfg_mgr	Sets the syslog filter level for FabricPath configuration manager.
fc2d	Sets level for fc2d syslog messages.
fcdomain	Sets level for fcdomain syslog messages.
fcns	Sets syslog filter level for name server.
fcoe_mgr	Sets the level for Fibre Channel over Ethernet (FCoE) manager syslog messages.
fcpc	Sets level for fcpc syslog messages.
fcs	Sets syslog filter level for FCS.
fdmi	Sets logging level for fdmi.
feature-mgr	Feature manager syslog level.
fex	Sets the level for Cisco Nexus 2000 Series Fabric Extender syslog messages.
flexlink	Sets level for switchport backup syslog messages.
flogi	Configure level for flogi syslog messages.
fs-daemon	FS daemon syslog level.
fspf	FSPF syslog level.
ftp	Sets level for File Transfer System.
fwm	Sets level for fwm syslog messages.
gatos	Gatos syslog level.
im	Sets level for im syslog messages.
interface-vlan	Sets level for interface VLAN syslog messages.
ip	Sets level for IP syslog messages.
ipconf	Sets level for ipconf syslog messages.
ipqos	Sets level for ipqosmgr syslog messages.
kernel	Sets level for kernel.
l3vm	Sets syslog filter level for L3VM.
lacp	Sets level for LACP syslog messages.
license	Licensing syslog level. Note This facility was deprecated and replaced with the licmgr facility in Cisco NX-OS 5.0(2)N1(1). For backwards compatibility, it will be maintained for a number of releases.
licmgr	Licensing syslog level.

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

Table 1-1 System Message Logging Facilities (continued)

Facility	Description
lldp	Sets level for LLDP syslog messages.
local0	Sets level for Local use daemons.
local1	Sets level for Local use daemons.
local2	Sets level for Local use daemons.
local3	Sets level for Local use daemons.
local4	Sets level for Local use daemons.
local5	Sets level for Local use daemons.
local6	Sets level for Local use daemons.
local7	Sets level for Local use daemons.
lpr	Sets level for Line Printer System.
m2rib	Sets level for Multicast Routing Information Base (MRIB) logging messages.
mail	Sets level for Mail system.
mfdm	Sets level for multicast Forwarding Information Base (FIB) distribution (MFDm) syslog messages.
mfwd	Sets level for multicast forwarding system messages.
monitor	Sets level for ethernet Switched Port Analyzer (SPAN) syslog messages.
news	Sets level for USENET news.
nohms	Sets level for nohms syslog messages.
nqosm	Sets level for nqosm syslog messages.
ntp	Sets syslog filter level for NTP.
pfm	Sets level for pfm syslog messages.
pktmgr	Sets syslog filter level for Packet Manager.
plugin	Sets level for plugin syslog messages.
port	Sets level for port syslog messages.
port-channel	Sets level for EtherChannel syslog messages.
port-profile	Sets level for port profile syslog messages.
port-resources	Sets level for prm syslog messages.
provision	Sets level for provision syslog messages.
qd	Sets level for qd syslog messages.
radius	RADIUS syslog level.
rdl	Sets logging level for RDL.
res_mgr	Set slevel for res_mgr syslog messages.
rib	Sets level for rib.
rlir	Sets level for RLIR.
routing	Sets level for routing information.

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

Table 1-1 System Message Logging Facilities (continued)

Facility	Description
rscn	Sets level for RSCN.
san-port-channel	Sets level for san-port-channel syslog messages.
scsi-target	SCSI target daemon syslog level.
security	Security syslog level.
session	Sets level for session-manager syslog messages. Note This facility was deprecated and replaced with the session-mgr facility in Cisco NX-OS 5.0(2)N1(1). For backward compatibility, it will be maintained for a number of releases.
session-mgr	Sets level for session-manager syslog messages.
smm	Sets logging level for Shared Memory Manager.
snmpd	Sets level for SNMP syslog messages.
sifmgr	Sets level for sifmgr syslog messages.
spanning-tree	Sets level for stp syslog messages.
stp	Sets level for stp syslog messages.
syslog	Sets level for Internal Syslog Messages.
sysmgr	System Manager syslog level.
tacacs	TACACS+ syslog level.
track	Sets level for object tracking messages.
tcpudp	Sets syslog filter level for TCPUDP.
track	Sets level for track syslog messages.
udld	Sets level for UDLD syslog messages.
ufdm	Sets level for unicast Forwarding Information Base (FIB) distribution (UFDM) syslog messages.
urib	Sets syslog filter level for Unicast Routing Information Base (URIB).
user	Sets level for User Process.
uucp	Sets level for Unix-to-Unix copy system.
vlan_mgr	Sets level for VLAN syslog messages.
vmm	Sets level for vmm syslog messages.
vpc	Sets level for vPC syslog messages.
vsan	VSAN syslog level.
vshd	Sets logging level for vshd.
vtp	Sets level for interface vlan syslog messages.
wwnm	Sets WWN Manager syslog level.
xml	XML agent syslog level.
zone	Sets syslog filter level for zone server.
zschk	Sets level for zschk syslog messages.