



Send comments to nexus3k-docfeedback@cisco.com



Cisco Nexus 3000 Series NX-OS System Management Command Reference

First Published: April 2011

Last Modified: September 2015

Cisco Systems, Inc.

www.cisco.com

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

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

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

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

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

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

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

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



Preface 1

Audience	1
Document Conventions	1
Related Documentation	2
Documentation Feedback	3
Obtaining Documentation and Submitting a Service Request	13

New and Changed Information 115

System Management Commands 11

abort (Call Home)	12
abort (session)	13
action cli	14
action counter	16
action event-default	18
action policy-default	110
action reload	112
action snmp-trap	114
action syslog	116
alert-group (Call Home)	118
callhome	120
callhome send diagnostic	121
callhome test	122
clear counters mpls strip	123
clear logging logfile	125
clear logging nvram	126
clear logging onboard	127
clear logging session	128
clear mpls strip label dynamic	129
clear ntp session	131
clear ntp statistics	132

Send comments to nexus3k-docfeedback@cisco.com

clear ptp counters	133
clear scheduler logfile	134
clear sflow statistics	135
clock protocol	136
commit (Call Home)	137
commit (session)	138
contract-id (Call Home)	139
customer-id (Call Home)	140
description	141
description (SPAN, ERSPAN)	142
destination ip (ERSPAN)	144
destination interface (ERSPAN)	145
destination-profile (Call Home)	146
diagnostic bootup level	149
duplicate-message throttle (Call Home)	150
email-contact (Call Home)	151
enable (Call Home)	152
event cli	154
event counter	155
event fanabsent	157
event fanbad	158
event manager applet	159
event manager environment	160
event manager policy	161
event manager policy internal	162
event memory	163
event oir	164
event policy-default	165
event snmp	166
event storm-control	169
event syslog	170
event sysmgr	172
event temperature	174
event track	175
feature ntp	176

Send comments to nexus3k-docfeedback@cisco.com

feature ptp	177
feature scheduler	179
feature sflow	180
filter access-group	181
hardware profile buffer info port-threshold	182
hardware profile parity-error	183
hardware profile tap-aggregation	185
hardware profile unicast syslog host-table-detail	186
ip access-list (session)	188
ip domain-list	189
ip domain-lookup	191
ip domain-name	192
ip host	194
ip name-server	195
ip port access-group (session)	197
logging abort	198
logging commit	199
logging console	1100
logging distribute	1101
logging event	1102
logging event port	1103
logging ip access-list cache entries num_entries	1104
logging ip access-list cache interval seconds	1105
logging ip access-list cache threshold num_packets	1106
logging level	1107
logging logfile	1109
logging module	1111
logging monitor	1112
logging server	1113
logging source-interface	1115
logging timestamp	1117
mode tap-aggregation	1118
monitor erspan origin ip-address	1119
monitor session	1120
mpls strip dest-mac	1122

Send comments to nexus3k-docfeedback@cisco.com

mpls strip	1123
mpls strip label	1124
mpls strip label-age	1126
ntp	1127
ntp abort	1129
ntp access-group	1130
ntp authenticate	1132
ntp authentication-key	1134
ntp broadcast	1135
ntp broadcastdelay	1136
ntp commit	1137
ntp disable	1138
ntp distribute	1139
ntp logging	1140
ntp master	1142
ntp multicast	1144
ntp multicast client	1146
ntp peer	1148
ntp server	1149
ntp source	1150
ntp source-interface	1151
ntp sync-retry	1152
ntp trusted-key	1153
periodic-inventory (Call Home)	1154
phone-contact (Call Home)	1156
ptp	1157
ptp announce	1158
ptp delay-request minimum interval	1160
ptp domain	1162
ptp priority1	1163
ptp priority2	1164
ptp source	1165
ptp sync interval	1167
ptp vlan	1169
rmon alarm	1171

Send comments to nexus3k-docfeedback@cisco.com

rmon event	1173
rmon hcalarm	1175
scheduler	1177
sflow agent-ip	1179
sflow collector-ip	1180
sflow collector-port	1181
sflow counter-poll-interval	1182
sflow data-source	1183
sflow max-datagram-size	1185
sflow max-sampled-size	1186
sflow sampling-rate	1187
show callhome	1188
show callhome destination-profile	1189
show callhome transport-email	1191
show callhome user-def-cmds	1192
show diagnostic bootup level	1193
show diagnostic result	1194
show event manager environment	1195
show event manager event-types	1197
show event manager history events	1200
show event manager policy-state	1202
show event manager script system	1204
show event manager system-policy	1205
show forwarding mpls stats	1208
show hardware forwarding memory health summary	1209
show hosts	1210
show logging console	1211
show logging info	1212
show logging last	1213
show logging level	1214
show logging logfile	1216
show logging module	1217
show logging monitor	1218
show logging nvram	1219
show logging onboard	1220

Send comments to nexus3k-docfeedback@cisco.com

show logging pending	1224
show logging pending-diff	1225
show logging session status	1226
show logging server	1227
show logging status	1228
show logging timestamp	1229
show monitor session	1230
show mpls strip labels	1233
show ntp access-groups	1235
show ntp authentication-keys	1236
show ntp authentication-status	1237
show ntp logging-status	1238
show ntp peers	1239
show ntp peer-status	1240
show ntp pending-diff	1241
show ntp pending peers	1242
show ntp session status	1243
show ntp status	1244
show ntp source	1245
show ntp source-interface	1246
show ntp statistics	1247
show ntp status	1248
show ntp trusted-keys	1249
show ptp brief	1250
show ptp clock	1251
show ptp clock foreign-masters-record	1253
show ptp corrections	1255
show ptp parent	1256
show ptp port	1258
show ptp time-property	1260
show rmon	1261
show running-config	1263
show running-config callhome	1265
show running-config eem	1266
show running-config exclude-provision	1268

Send comments to nexus3k-docfeedback@cisco.com

show running-config interface	1270
show running-config monitor	1271
show running-config ptp	1273
show scheduler	1275
show sflow	1277
show sflow statistics	1278
show snmp community	1279
show snmp context	1280
show snmp engineID	1281
show snmp group	1282
show snmp host	1283
show snmp sessions	1284
show snmp trap	1285
show snmp user	1286
show startup-config	1287
show startup-config callhome	1288
show startup-config eem	1289
show startup-config exclude-provision	1291
show startup-config ptp	1292
show startup-config vtp	1294
show tech-support callhome	1295
shut (ERSPAN)	1296
site-id (Call Home)	1297
snmp-server community	1298
snmp-server contact	1300
snmp-server context	1301
snmp-server enable traps	1303
snmp-server enable traps link	1306
snmp-server enable traps vtp	1308
snmp-server globalEnforcePriv	1309
snmp-server host	1310
snmp-server location	1312
snmp-server mib community-map	1313
snmp-server tcp-session	1315
snmp-server user	1316

Send comments to nexus3k-docfeedback@cisco.com

snmp trap link-status	1318
source (SPAN, ERSPAN)	1320
source ip (ERSPAN)	1322
streetaddress (Call Home)	1323
switching-mode store-forward	1324
switchport mode monitor buffer-limit	1325
switch-priority (Call Home)	1326
tag	1327
terminal event-manager bypass	1329
transport email (Call Home)	1330
verify (session)	1332
vrf (ERSPAN)	1333



Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 3000 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 1](#)
- [Document Conventions, page 1](#)
- [Related Documentation, page 2](#)
- [Obtaining Documentation and Submitting a Service Request, page 3](#)

Audience

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

Document Conventions

Command descriptions use these conventions:

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

Screen examples use these conventions:

screen font	Terminal sessions and information that the switch displays are in screen font.
boldface screen font	Information that you must enter is in boldface screen font.

<i>italic screen font</i>	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:



Note

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



Caution

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

Related Documentation

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

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

The documentation set is divided into the following categories:

Release Notes

The release notes are available at the following URL:

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

Installation and Upgrade Guides

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

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

Command References

The command references are available at the following URL:

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

Technical References

The technical references are available at the following URL:

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

Configuration Guides

The configuration guides are available at the following URL:

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

Send comments to nexus3k-docfeedback@cisco.com

Error and System Messages

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

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

Documentation Feedback

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

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* at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Send comments to nexus3k-docfeedback@cisco.com



New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 3000 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/ps11541/tsd_products_support_series_home.html

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

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

Table 1 summarizes the new and changed features for Cisco NX-OS and tells you where they are documented.

Table 1 **New and Changed Information**

Feature	Description	Changed in Release	Where Documented
Precision time protocol	The sync interval range is now 2 to 4.	7.0(3)I2(1)	ptp sync interval
Precision time protocol	The announce timeout range is now 2 to 4.	7.0(3)I2(1)	ptp announce
Show monitor session	The number of TCAM entries available for ACL SPAN has been reduced by 6 entries.	7.0(3)I2(1)	show monitor session
show logging onboard	While the induced errors are corrected on the switches, the log messages that notify the corrections stop after hitting a threshold (usually after 15 or 19 corrections). Also, an extra message gets printed when the parity error is injected.	7.0(3)I2(1)	show logging onboard
Show monitor session	The option for filter VLANs has been removed. This feature now displays rx, tx, and both for the source VLANs.	7.0(3)I2(1)	show monitor session
Snmp-server contact	This command no longer has a default name and must be configured to enable callhome.	7.0(3)I2(1)	snmp-server contact

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

Table 1 **New and Changed Information**

Feature	Description	Changed in Release	Where Documented
Clear sflow statistics	This command no longer clears the Total Samples and Dropped Samples fields. To clear Total Samples: clear hardware rate-limiter sflow To clear Total Packets: clear hardware rate-limiter sflow	7.0(3)I2(1)	clear sflow statistics
Clock protocol	This command will no longer set the clock. To change the clock manually, see the <i>Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide</i> .	7.0(3)I2(1)	clock protocol
Syslog for ALPM mode	A new CLI command [no] hardware profile unicast syslog host-table-detail has been added.	6.0(2)U5(4)	hardware profile unicast syslog host-table-detail
ERSPAN Enhancements	The egress interface information is added for the ERSPAN source session in the show monitor session <session-number> command..	6.0(2)U5(1)	show monitor session
MPLS output statistics	The MPLS output statistics are displayed in show forwarding mpls stats command.	6.0(2)U5(1)	show forwarding mpls stats
MPLS Stripping	This feature was introduced.	6.0(2)U2(5)	clear counters mpls strip clear mpls strip label dynamic mpls strip dest-mac mpls strip mpls strip label mpls strip label-age show mpls strip labels
Tap Aggregation	This feature was introduced.	6.0(2)U2(3)	hardware profile parity-error mode tap-aggregation
Soft Error Recovery	This feature was introduced.	6.0(2)U2(1)	show hardware forwarding memory health summary
NTP Server	This feature was introduced.	6.0(2)U2(1)	feature ntp mpls strip dest-mac ntp access-group ntp master ntp broadcast ntp multicast
SPAN with ACL filtering	This feature was introduced.	6.0(2)U2(1)	filter access-group
Configurable SPAN buffer limit	This feature was introduced.	5.0(3)U5(1)	switchport mode monitor buffer-limit

Send comments to nexus3k-docfeedback@cisco.com

Table 1 ***New and Changed Information***

Feature	Description	Changed in Release	Where Documented
Syslog user-configurable source-IP	This feature was introduced.	5.0(3)U5(1)	logging source-interface
sFLOW	This feature was introduced.	5.0(3)U4(1)	clear sflow statistics feature sflow sflow agent-ip sflow collector-ip sflow collector-port sflow counter-poll-interval sflow data-source sflow max-datagram-size sflow max-sampled-size sflow sampling-rate show sflow show sflow statistics
Syslog Thresholds for System Resources	This feature was introduced.	5.0(3)U3(2)	filter access-group
Store and Forward Switching	This feature was introduced.	5.0(3)U3(1)	switching-mode store-forward
Scheduler	This feature was introduced.	5.0(3)U3(1)	clear scheduler logfile feature scheduler scheduler show scheduler
Quad Small Form-factor Pluggable (QSFP+) Port	Updated the filter access-group command.	5.0(3)U3(1)	filter access-group

Send comments to nexus3k-docfeedback@cisco.com

Table 1 ***New and Changed Information***

Feature	Description	Changed in Release	Where Documented
Embedded Event Manager	This feature was introduced.	5.0(3)U3(1)	action cli action counter action event-default action policy-default action reload action snmp-trap action syslog description event cli event counter event fanabsent event fanbad event manager applet event manager environment event manager policy event manager policy internal event memory event oir event policy-default event snmp event storm-control event syslog event sysmgr event temperature event track show event manager environment show event manager event-types show event manager history events show event manager policy-state show event manager script system show event manager system-policy show running-config eem show startup-config eem tag terminal event-manager bypass

Send comments to nexus3k-docfeedback@cisco.com

Table 1 ***New and Changed Information***

Feature	Description	Changed in Release	Where Documented
ERSPAN	This feature was introduced. The monitor session command was updated to include the erspan-destination and erspan-source keywords.	5.0(3)U2(2)	description (SPAN, ERSPAN) destination ip (ERSPAN) destination interface (ERSPAN) monitor erspan origin ip-address monitor session shut (ERSPAN) source (SPAN, ERSPAN) source ip (ERSPAN) vrf (ERSPAN) show monitor session show running-config monitor
Precision Time Protocol (PTP)	This feature was introduced.	5.0(3)U2(2)	clear ptp counters clock protocol feature ntp ptp ptp announce ptp delay-request minimum interval ptp domain ptp priority1 ptp priority2 ptp source ptp sync interval ptp vlan show ntp trusted-keys show ptp clock show ptp clock foreign-masters-record show ptp corrections show ptp parent show ptp port show ptp time-property show running-config ptp show startup-config ptp

Send comments to nexus3k-docfeedback@cisco.com

Table 1 ***New and Changed Information***

Feature	Description	Changed in Release	Where Documented
40-Gigabit Ethernet Quad small form-factor pluggable (QSFP+) port	<p>This feature was introduced to support 40-Gigabit Ethernet on QSFP+ ports.</p> <p>The following command was added in this release:</p> <ul style="list-style-type: none"> hardware profile portmode 	5.0(3)U2(1)	filter access-group
Domain Name System (DNS)	<p>This feature was introduced.</p> <p>You can configure a DNS host, server, or name and enable the DNS lookup feature.</p>	5.0(3)U1(1)	ip domain-list ip domain-lookup ip domain-name ip host ip name-server show hardware forwarding memory health summary
Network Time Protocol (NTP)	<p>This feature was introduced.</p> <p>You can configure NTP peers and servers.</p>	5.0(3)U1(1)	mpls strip dest-mac ntp abort ntp access-group ntp disable ntp logging show mpls strip labels show ntp pending-diff show ntp pending-diff show ntp status

Send comments to nexus3k-docfeedback@cisco.com

Table 1 ***New and Changed Information***

Feature	Description	Changed in Release	Where Documented
Call Home	<p>This feature was introduced.</p> <p>You can configure the Cisco Smart Call Home service and parameters on a Cisco NX-OS switch.</p>	5.0(3)U1(1)	<p>abort (Call Home)</p> <p>alert-group (Call Home)</p> <p>callhome</p> <p>callhome send diagnostic</p> <p>callhome test</p> <p>commit (Call Home)</p> <p>contract-id (Call Home)</p> <p>customer-id (Call Home)</p> <p>destination-profile (Call Home)</p> <p>duplicate-message throttle (Call Home)</p> <p>email-contact (Call Home)</p> <p>enable (Call Home)</p> <p>ntp trusted-key</p> <p>phone-contact (Call Home)</p> <p>show callhome</p> <p>show callhome destination-profile</p> <p>show callhome transport-email</p> <p>show callhome user-def-cmds</p> <p>show running-config callhome</p> <p>show startup-config callhome</p> <p>show tech-support callhome</p> <p>site-id (Call Home)</p> <p>streetaddress (Call Home)</p> <p>switch-priority (Call Home)</p> <p>transport email (Call Home)</p>

Send comments to nexus3k-docfeedback@cisco.com

Table 1 ***New and Changed Information***

Feature	Description	Changed in Release	Where Documented
Simple Network Management Protocol (SNMP)	This feature was introduced. You can configure an SNMP server and trap, or enable SNMP notifications for a VTP domain.	5.0(3)U1(1)	snmp-server community 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 community show snmp context show snmp engineID show snmp group show snmp host show snmp sessions show snmp trap show snmp user
Virtual forwarding and routing (VRF)	This feature was introduced. You can configure VRF, VRF-lite features, and the IP features for a VRF.	5.0(3)U1(1)	ip domain-list ip domain-lookup ip domain-name ip host ip name-server show hardware forwarding memory health summary

Send comments to nexus3k-docfeedback@cisco.com

Table 1 ***New and Changed Information***

Feature	Description	Changed in Release	Where Documented
System Management	You can use the system management commands to enable logging messages, configure a remote syslog server, or verify a session configuration.	5.0(3)U1(1)	abort (session) clear counters mpls strip clear logging nvram clear logging onboard clear logging session clear mpls strip label dynamic clear ntp statistics commit (session) diagnostic bootup level ip access-list (session) ip port access-group (session) logging abort logging commit logging console logging distribute logging event logging event port logging logfile logging module logging monitor logging server logging timestamp show diagnostic bootup level show diagnostic result show hardware forwarding memory health summary show logging console show logging info show logging last show logging level show logging logfile show logging module show logging monitor show logging nvram

Send comments to nexus3k-docfeedback@cisco.com

Table 1 ***New and Changed Information***

Feature	Description	Changed in Release	Where Documented
System Management (continued)			show logging onboard show logging pending show logging pending-diff show logging session status show logging server show logging status show logging timestamp verify (session)
Remote Monitoring (RMON)	This feature was introduced. You can configure RMON alarms on a Cisco NX-OS switch.	5.0(3)U1(1)	rmon alarm rmon event rmon hcalarm show rmon



System Management Commands

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

Send comments to nexus3k-docfeedback@cisco.com

abort (Call Home)

To discard Call Home configuration changes and release the Cisco Fabric Services (CFS) lock, use the **abort** command.

abort

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

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

Command Modes	Callhome configuration mode
----------------------	-----------------------------

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

Usage Guidelines	Use this command if you are the CFS lock owner or if you are logged into the device that holds the CFS lock.
-------------------------	--

Examples	This example shows how to discard Call Home configuration changes:
-----------------	--

```
switch(config-callhome)# abort
switch(config-callhome)#
```

Related Commands	Command	Description
	show callhome	Displays Call Home configuration information.
	show running-config callhome	Displays the running configuration information for Call Home.

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

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

<pre>switch# configure session MySession1 switch(config-s)# abort switch#</pre>

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 nexus3k-docfeedback@cisco.com

action cli

To configure a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered, use the **action cli** command. To disable the VSH command string, use the **no** form of this command.

action *label num1* [.num2] **cli** [**local**] *vsh_cmd*

no action *label num1* [.num2] **cli**

Syntax Description

<i>label num1</i> [.num2]	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the <i>label</i> as the sort key. The range for num1 is from 1 to 16 and the range for num2 is from 0 to 9.
local	(Optional) Specifies the action is to be executed in the same module on which the event occurs.
<i>vsh_cmd</i>	VSH command string to be executed when the applet is triggered.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a VSH command string to be executed when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet cli-applet
switch(config-applet)# action 1.1 cli show version
switch(config-applet)#
```

Related Commands

Command	Description
action counter	Sets or modifies a named counter when an Embedded Event Manager (EEM) applet is triggered.
action event-default	Specifies that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered.
action policy-default	Enables the default action of the policy being overridden.

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
action reload	Specifies the action of reloading the Cisco Nexus 3000 Series software when an Embedded Event Manager (EEM) applet is triggered.
action snmp-trap	Specifies the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered.
action syslog	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

Send comments to nexus3k-docfeedback@cisco.com

action counter

To set or modify a named counter when an Embedded Event Manager (EEM) applet is triggered, use the **action counter** command. To restore the default value to the counter, use the **no** form of this command.

action *label num1* [*.num2*] **counter name** *name* **value** *value* **op** {**dec** | **inc** | **nop** | **set**}

no action *label num1* [*.num2*] **counter name** *name*

Syntax Description

<i>label num1</i> [<i>.num2</i>]	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the <i>label</i> as the sort key. The range for <i>num1</i> is from 1 to 16 and the range for <i>num2</i> is from 0 to 9.
name <i>name</i>	Specifies the name of the counter. This identifier can be any string value up to 28 characters.
value <i>value</i>	Specifies the value of the counter. This identifier must be an integer value and can be in the range of 0 to 2147483647 or a \$-prefixed name (for parameter substitution).
op	Specifies the operation to perform upon the counter.
dec	Decrements the counter by the specified value.
inc	Increments the counter by the specified value.
nop	Does nothing; using this keyword just displays the specified value.
set	Sets the counter to the specified value.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to set the counter *count1* to the value in *\$variable* when the EEM counter-applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet counter-applet
switch(config-applet)# action 1.2 counter name count1 value $variable op dec
switch(config-applet)#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	action cli	Configures a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered.
	action event-default	Specifies that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered.
	action policy-default	Enables the default action of the policy being overridden.
	action reload	Specifies the action of reloading the Cisco Nexus 3000 Series software when an Embedded Event Manager (EEM) applet is triggered.
	action snmp-trap	Specifies the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered.
	action syslog	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

action event-default

To specify that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered, use the **action event-default** command. To disable the default action, use the **no** form of this command.

action *label num1* [*.num2*] **event-default**

no action *num1* [*.num2*] **event-default**

Syntax Description

label num1 [*.num2*] Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the *label* as the sort key. The range for *num1* is from 1 to 16 and the range for *num2* is from 0 to 9.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

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

Usage Guidelines

If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the **event-default** statement to the EEM policy or EEM does not allow the CLI command to execute. You can use the **terminal event-manager bypass** command to allow all EEM policies with CLI matches to execute the CLI command.

This command does not require a license.

Examples

This example shows how to specify that the default action for the event is to be performed when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet default-applet
switch(config-applet)# action 1.1 event-default
switch(config-applet)#
```

Related Commands

Command	Description
action cli	Configures a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered.
action counter	set or modify a named counter when an Embedded Event Manager (EEM) applet is triggered.

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
action policy-default	Enables the default action of the policy being overridden.
action reload	Specifies the action of reloading the Cisco Nexus 3000 Series software when an Embedded Event Manager (EEM) applet is triggered.
action snmp-trap	Specifies the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered.
action syslog	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

Send comments to nexus3k-docfeedback@cisco.com

action policy-default

To enable the default action of the policy being overridden, use the **action policy-default** command. To remove the default action, use the **no** form of this command.

action *label num1* [*.num2*] **policy-default**

no action *label num1* [*.num2*] **policy-default**

Syntax Description

label num1 [*.num2*] Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the *label* as the sort key. The range for *num1* is from 1 to 16 and the range for *num2* is from 0 to 9.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable the default action of a policy being overridden when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet default-applet
switch(config-applet)# action 1.0 policy-default
switch(config-applet)#
```

Related Commands

Command	Description
action cli	Configures a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered.
action counter	set or modify a named counter when an Embedded Event Manager (EEM) applet is triggered.
action event-default	Specifies that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered.
action reload	Specifies the action of reloading the Cisco Nexus 3000 Series software when an Embedded Event Manager (EEM) applet is triggered.

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
action snmp-trap	Specifies the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered.
action syslog	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

Send comments to nexus3k-docfeedback@cisco.com

action reload

To specify the action of reloading the Cisco Nexus 3000 Series switch software when an Embedded Event Manager (EEM) applet is triggered, use the **action reload** command. To remove the action of reloading the Cisco Nexus 3000 Series switch software, use the **no** form of this command.

action *label num1* [*.num2*] **reload**

no action *label num1* [*.num2*] **reload**

Syntax Description

label num1 [*.num2*] Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the *label* as the sort key. The range for *num1* is from 1 to 16 and the range for *num2* is from 0 to 9.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify the action of reloading the Cisco Nexus 3000 Series switch software when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet reload-applet
switch(config-applet)# action 1.5 reload
switch(config-applet)#
```

Related Commands

Command	Description
action cli	Configures a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered.
action counter	set or modify a named counter when an Embedded Event Manager (EEM) applet is triggered.
action event-default	Specifies that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered.
action policy-default	Enables the default action of the policy being overridden.

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
action snmp-trap	Specifies the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered.
action syslog	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

Send comments to nexus3k-docfeedback@cisco.com

action snmp-trap

To specify the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered, use the **action snmp-trap** command. To disable the SNMP trap, use the **no** form of this command.

action *label num1* [*.num2*] **snmp-trap** [*intdata1 integer*] [*intdata2 integer*] [*strdata string*]

no action *label num1* [*.num2*] **snmp-trap** [*intdata1 integer*] [*intdata2 integer*] [*strdata string*]

Syntax Description

<i>label num1</i> [<i>.num2</i>]	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the <i>label</i> as the sort key. The range for <i>num1</i> is from 1 to 16 and the range for <i>num2</i> is from 0 to 9.
intdata1 <i>integer</i>	(Optional) Specifies an integer to be sent in the SNMP trap message to the SNMP agent. The <i>integer</i> can be any number up to 80 characters.
intdata2 <i>integer</i>	(Optional) Specifies a second integer to be sent in the SNMP trap message to the SNMP agent. The second <i>integer</i> can be any number up to 80 characters.
strdata <i>string</i>	(Optional) Specifies a string to be sent in the SNMP trap message to the SNMP agent. If the string contains embedded blanks, enclose it in double quotation marks. The <i>string</i> can be any alphanumeric string up to 80 characters.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify an SNMP trap to generate when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet snmp-applet
switch(config-applet)# action 1.7 snmp-trap strdata "EEM detected server failure"
switch(config-applet)#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	action cli	Configures a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered.
	action counter	Sets or modifies a named counter when an Embedded Event Manager (EEM) applet is triggered.
	action event-default	Specifies that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered.
	action policy-default	Enables the default action of the policy being overridden.
	action reload	Specifies the action of reloading the Cisco Nexus 3000 Series software when an Embedded Event Manager (EEM) applet is triggered.
	action syslog	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

Send comments to nexus3k-docfeedback@cisco.com

action syslog

To configure a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered, use the **action syslog** command. To disable the syslog message, use the **no** form of this command.

action *label num1* [.num2] **syslog** [**priority** {*priority* | *priority-string*}] **msg** *message-text*

no action *label num1* [.num2] **syslog** [**priority** {*priority* | *priority-string*}] **msg** *message-text*

Syntax Description

<i>label num1</i> [.num2]	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric sequence using the <i>label</i> as the sort key. The range for num1 is from 1 to 16 and the range for num2 is from 0 to 9.
priority	(Optional) Specifies the priority level of the syslog messages. If this keyword is not selected, all syslog messages are set at the informational priority level. If this keyword is selected, the priority level argument must be defined.
<i>priority</i>	Priority level as follows: <ul style="list-style-type: none"> • emergencies—Specifies the system is unusable. • alerts—Specifies immediate action is needed. • critical—Specifies critical conditions. • errors—Specifies error conditions. • warnings—Specifies warning conditions. • notifications—Specifies normal but significant conditions. • informational—Specifies informational messages. This is the default. • debugging—Specifies debugging messages.
<i>priority-string</i>	\$-prefixed parameter that you previously set to a priority level.
msg <i>message-text</i>	Specifies the message to be logged. The <i>message-text</i> can contain any alphanumeric string up to 256 characters.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

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

Usage Guidelines

Messages written to the syslog from an EEM applet are not screened for EEM syslog events, which might lead to recursive EEM syslog events. Messages that are sent from an EEM applet include the applet name for identification.

This command does not require a license.

Send comments to nexus3k-docfeedback@cisco.com

Examples

This example shows how to configure a syslog message to save when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet syslog-applet
switch(config-applet)# action 1.7 syslog priority critical msg cpu usage high
switch(config-applet)#
```

Related Commands

Command	Description
action cli	Configures a virtual shell (VSH) command string to be executed when an Embedded Event Manager (EEM) applet is triggered.
action counter	set or modify a named counter when an Embedded Event Manager (EEM) applet is triggered.
action event-default	Specifies that the default action for the event is to be performed when an Embedded Event Manager (EEM) applet is triggered.
action policy-default	Enables the default action of the policy being overridden.
action reload	Specifies the action of reloading the Cisco Nexus 3000 Series software when an Embedded Event Manager (EEM) applet is triggered.
action snmp-trap	Specifies the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered.

Send comments to nexus3k-docfeedback@cisco.com

alert-group (Call Home)

To configure a CLI **show** command for an alert group, use the **alert-group** command. To remove a CLI command from an alert group, use the **no** form of this command.

alert-group *alert user-def-cmd CLI-command*

no alert-group *alert user-def-cmd CLI-command*

Syntax Description	<i>alert</i>	Alert group. The <i>alert</i> group can be one of the following:
		<ul style="list-style-type: none"> • All—All alert groups • Cisco-TAC—Cisco TAC events • Configuration—Configuration events • Diagnostic—Diagnostic events • EEM—EEM events • Environmental—Power, fan, temperature-related events • Inventory—Inventory status events • License—Licensing events • Linecard-Hardware—Linecard-related events • Supervisor-Hardware—Supervisor-related events • Syslog-group-port—Syslog message events filed by port manager • System—Software-related events • Test—User-generated test events
	user-def-cmd	Specifies a CLI command for an alert group.
	<i>CLI-command</i>	CLI show command. The command can be a maximum of 512 characters.

Command Default None

Command Modes Callhome configuration mode

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

Usage Guidelines You can customize predefined alert groups to execute additional CLI **show** commands when specific events occur and send that **show** output with the Call Home message. You can assign a maximum of five user-defined CLI show commands to an alert group.

You must enclose the **show** command in double quotes. Only valid show commands are accepted.

Send comments to nexus3k-docfeedback@cisco.com

**Note**

You cannot add user-defined CLI **show** commands to the CiscoTAC-1 destination profile.

You can add **show** commands only to full text and XML destination profiles. Short text destination profiles do not support additional **show** commands because they only allow 128 bytes of text.

Examples

This example shows how to add a **show** command output to a Call Home message sent for an alert group:

```
switch(config-callhome)# alert-group configuration user-def-cmd "show running-config"
switch(config-callhome)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves this configuration change.
show callhome user-def-cmd	Displays information about all user-defined show commands added to alert groups.

Send comments to nexus3k-docfeedback@cisco.com

callhome

To configure the Cisco Smart Call Home service and enter the callhome configuration mode, use the **callhome** command.

callhome

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration mode

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

Usage Guidelines You must configure the e-mail, phone, and street address information for Call Home. You can optionally configure the contract ID, customer ID, site ID, and switch priority information.

Examples This example shows how to enter callhome configuration mode:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)#
```

Related Commands	Command	Description
	email-contact	Configures the e-mail address.
	show callhome	Displays a summary of the Call Home configuration.
	snmp-server contact	Configures the SNMP contact (sysContact).

Send comments to nexus3k-docfeedback@cisco.com

callhome send diagnostic

To send a specified Call Home test message to all configured destinations, use the **callhome send diagnostic** command.

callhome send diagnostic

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

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

Command Modes	Callhome configuration mode
----------------------	-----------------------------

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

Usage Guidelines	You can generate a test message to test your Call Home communications using the callhome send diagnostic command.
-------------------------	--

Examples	This example shows how to configure Call Home to send test messages to all configured destinations:
-----------------	---

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# callhome send diagnostic
switch(config-callhome)#
```

Related Commands	Command	Description
	show callhome	Displays Call Home configuration information.
	show running-config callhome	Displays the running configuration information for Call Home.

Send comments to nexus3k-docfeedback@cisco.com

callhome test

To send a Call Home test message to all configured destinations, use the **callhome test** command.

callhome test [inventory]

Syntax Description	inventory	(Optional) Specifies that a Call Home inventory message be sent for testing the Call Home configuration.
--------------------	-----------	--

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

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

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

Examples This example shows how to send a Call Home test message to all configured destinations:

```
switch# callhome test
trying to send test callhome message
successfully sent test callhome message
switch#
```

This example shows how to send a Call Home inventory message to all configured destinations:

```
switch# callhome test inventory
trying to send test callhome inventory message
successfully sent test callhome inventory message
switch#
```

Related Commands	Command	Description
	show callhome	Displays Call Home configuration information.
	show running-config callhome	Displays the running configuration information for Call Home.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

clear counters mpls strip

To clear all software and hardware MPLS stripping counters, use the **clear counters mpls strip** command.

clear counters mpls strip

Syntax Description This command has no arguments or keywords

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	6.0(2)U2(5)	This command was introduced.

Examples This example shows how to clear all MPLS stripping counters:

```
switch# clear counters mpls strip
```

```
switch# show mpls strip labels
```

```
MPLS Strip Labels:
```

```
Total      : 15000
```

```
Static     : 2
```

```
Legend:    * - Static Label
```

```
Interface - where label was first learned
```

```
Idle-Age   - Seconds since last use
```

```
SW-Counter- Packets received in Software
```

```
HW-Counter- Packets switched in Hardware
```

Label	Interface	Idle-Age	SW-Counter	HW-Counter
4096	Eth1/44	15	0	0
8192	Eth1/44	17	0	0
12288	Eth1/44	15	0	0
16384	Eth1/44	39	0	0
20480	Eth1/44	47	0	0
24576	Eth1/44	7	0	0
28672	Eth1/44	5	0	0
36864	Eth1/44	7	0	0
40960	Eth1/44	19	0	0
45056	Eth1/44	9	0	0
49152	Eth1/44	45	0	0
53248	Eth1/44	9	0	0

Related Commands	Command	Description
	mpls strip	Enables the MPLS stripping feature.
	mpls strip dest-mac	Configures the destination MAC address for stripped egress frames.

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
mpls strip label	Adds or deletes static MPLS labels.
mpls strip label-age	Configures MPLS label aging.
clear mpls strip label dynamic	Clears dynamic label entries.
show mpls strip labels	Displays MPLS label configuration.

Send comments to nexus3k-docfeedback@cisco.com

clear logging logfile

To clears 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
	5.0(3)U1(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 nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	This example shows how to clear the NVRAM logs:
-----------------	---

```
switch# clear logging nvram
switch#
```

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

Send comments to nexus3k-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-up/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
5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to clear the OBFL environmental history entries:

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

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

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

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

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

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

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

Related Commands

Command	Description
show logging onboard	Displays onboard failure logs.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	This example shows how to clear the current logging session:
	<pre>switch# clear logging session switch#</pre>

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

Send comments to nexus3k-docfeedback@cisco.com

clear mpls strip label dynamic

To clear dynamic label entries from the MPLS label table, use the **clear mpls strip label dynamic** command.

clear mpls strip label dynamic

Syntax Description This command has no arguments or keywords

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	6.0(2)U2(5)	This command was introduced.

Examples This example shows how to clear dynamic label entries:

```
switch(config)# sh mpls strip labels
MPLS Strip Labels:
```

```
Total      : 2
```

```
Static      : 0
```

```
Legend:      * - Static Label
```

```
Interface - where label was first learned
```

```
Idle-Age   - Seconds since last use
```

```
SW-Counter- Packets received in Software
```

```
HW-Counter- Packets switched in Hardware
```

```
-----
Label      Interface      Idle-Age   SW-Counter   HW-Counter
-----
450000     Eth1/47                1             2             0
45000      Eth1/47                1             1             0
```

```
switch(config)# clear mpls strip labels dynamic
```

```
switch(config)# sh mpls strip labels
```

```
MPLS Strip Labels:
```

Send comments to nexus3k-docfeedback@cisco.com

```

Total          : 0

Static         : 0
Legend:      * - Static Label

Interface - where label was first learned

Idle-Age  - Seconds since last use

SW-Counter- Packets received in Software

HW-Counter- Packets switched in Hardware

```

```

-----
Label      Interface      Idle-Age  SW-Counter  HW-Counter
-----

```

```
switch(config)#
```

Related Commands

Command	Description
mpls strip	Enables the MPLS stripping feature.
mpls strip dest-mac	Configures the destination MAC address for stripped egress frames.
mpls strip label	Adds or deletes static MPLS labels.
mpls strip label-age	Configures MPLS label aging.
show mpls strip labels	Displays MPLS label configuration.

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	This example shows how to discard the NTP distribution session in progress:
-----------------	---

```
switch# clear ntp session
switch#
```

Related Commands	Command	Description
	show ntp	Displays NTP information.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples This example shows how to discard the NTP I/O statistics:

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

Related Commands	Command	Description
	show ntp	Displays NTP information.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

clear ptp counters

To clear the Precision Time Protocol (PTP) packet counters, use the **clear ptp counters** command.

clear ptp counters {**all** | **interface ethernet** *slot/port*}

Syntax Description	all	Clears all PTP counters.
	interface	Clears PTP counters from an interface.
	ethernet <i>slot/port</i>	Clears PTP counters from an IEEE 802.3z Ethernet interface. The slot number is from 1 to 255 and the port number is from 1 to 128.

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

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

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines	This command does not require a license.
------------------	--

Examples	This example shows how to clear all PTP counters:
----------	---

```
switch# clear ptp counters all
switch#
```

Related Commands	Command	Description
	feature ptp	Enables PTP on the switch.
	show running-config ptp	Displays the PTP running system configuration information.

Send comments to nexus3k-docfeedback@cisco.com

clear scheduler logfile

To clear the scheduler log file, use the **clear scheduler logfile** command.

clear scheduler logfile

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

Defaults	None
-----------------	------

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

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

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	<p>This example shows how clear the scheduler log file:</p> <pre>switch# configure terminal switch(config)# clear scheduler logfile switch(config)#</pre>
-----------------	---

Related Commands	Command	Description
	show scheduler	Displays the scheduler configuration.

Send comments to nexus3k-docfeedback@cisco.com

clear sflow statistics

To clear the sFlow statistics, use the **clear sflow statistics** command.

clear sflow statistics



Note Beginning in Release 7.0(3)I2(1), the Total Samples and Total Samples fields are not cleared.

To clear Total Samples: **clear hardware rate-limiter sflow**

To clear Total Packets: **clear hardware rate-limiter sflow**

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Global configuration mode

Command History	Release	Modification
	5.0(3)U4(1)	This command was introduced.
	7.0(3)I2(1)	The Total Samples and Total Samples fields are not cleared.

Usage Guidelines This command does not require a license.

Examples This example shows how clear the sFlow statistics:

```
switch# configure terminal
switch(config)# clear sflow statistics
switch(config)#
```

Related Commands	Command	Description
	show sflow	Displays the sFlow configuration.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

clock protocol

To set the synchronization protocol for the clock to a protocol, use the **clock protocol** command. To remove the clock protocol, use the **no** form of this command.



Note Beginning in Release 7.0(3)I2(1), this command will not set the clock. To change the clock manually, see the *Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide*.

clock protocol {none | ntp | ptp}

no clock protocol {none | ntp | ptp}

Syntax Description

none	Specifies that the clock can be set manually.
ntp	Specifies that the clock be set to the Network Time Protocol (NTP).
ptp	Specifies that the clock be set to the Precision Time Protocol (PTP).

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U2(2)	This command was introduced.
7.0(3)I2(1)	This command will not set the clock

Usage Guidelines

This command does not require a license.

Examples

This example shows how to set the synchronization protocol for the clock to PTP:

```
switch# configure terminal
switch(config)# clock protocol ptp
switch(config)#
```

Related Commands

Command	Description
feature ptp	Enables PTP on the switch.
show ptp clock	Displays the PTP clock information.
show running-config ptp	Displays the PTP running system configuration information.

Send comments to nexus3k-docfeedback@cisco.com

commit (Call Home)

To commit Call Home configuration changes and distribute the changes to call Cisco Fabric Services (CFS)-enabled devices, use the **commit** command.

commit

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

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

Command Modes	Callhome configuration mode
----------------------	-----------------------------

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

Examples	This example shows how to commit CFS Call Home configuration changes:
-----------------	---

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# commit
switch(config-callhome)#
```

Related Commands	Command	Description
	show callhome	Displays Call Home configuration information.
	show running-config callhome	Displays the running configuration information for Call Home.

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples This example shows how to commit the current session:

```
switch# configure session MySession
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 nexus3k-docfeedback@cisco.com

contract-id (Call Home)

To configure the optional contract number for the customer, use the **contract-id** command. To remove a contract number, use the **no** form of this command.

contract-id *contract-number*

no contract-id

Syntax Description

<i>contract-number</i>	Contract number. The contract number can be up to 255 alphanumeric characters in free format.
------------------------	---

Command Default

None

Command Modes

Callhome configuration mode

Command History

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

Usage Guidelines

You can configure the customer identification information that Cisco Smart Call Home should use. The service agreement includes the customer identification information, such as the customer ID, contract ID, and site ID.

Examples

This example shows how to configure the contract number for the customer:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# contract-id 12095134-1706
switch(config-callhome)#
```

Related Commands

Command	Description
customer-id	Configures the customer number for the switch.
show callhome	Displays a summary of the Call Home configuration.

Send comments to nexus3k-docfeedback@cisco.com

customer-id (Call Home)

To configure the optional unique identification number for the customer, use the **customer-id** command. To remove a customer number, use the **no** form of this command.

customer-id *customer-no*

no customer-id

Syntax Description

<i>customer-no</i>	Customer number, as specified in the service agreement. The customer number can be up to 255 alphanumeric characters in free format.
--------------------	--

Command Default

None

Command Modes

Callhome configuration mode

Command History

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

Usage Guidelines

You can configure the customer identification information that Cisco Smart Call Home should use. The service agreement includes the customer identification information, such as the customer ID, contract ID, and site ID.

Examples

This example shows how to configure a customer number:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# customer-id AXC-1203
switch(config-callhome)#
```

Related Commands

Command	Description
site-id	Configures the site number for the switch.
show callhome	Displays a summary of the Call Home configuration.

Send comments to nexus3k-docfeedback@cisco.com

description

To add a description to a user policy, use the **description** command. To remove the policy description, use the **no** form of this command.

description *policy-description*

no description *policy-description*

Syntax Description

<i>policy-description</i>	Policy description. The description can be any case-sensitive, alphanumeric string up to 80 characters enclosed by quotation marks.
---------------------------	---

Defaults

None

Command Modes

Applet configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to add a description to a user policy:

```
switch# configure terminal
switch(config)# event manager applet monitorShutdown
switch(config-applet)# description "Monitors interface shutdown"
```

This example shows how to remove the policy description:

```
switch(config-applet)# no description "Monitors interface shutdown"
switch(config-applet)#
```

Related Commands

Command	Description
description	Configures a descriptive string for the policy.
event	Configures the event statement for the policy.
show event-manager policy state	Correlates multiple events in the policy.
tag	Displays information about the status of the configured policy.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

description (SPAN, ERSPAN)

To add a description to an Ethernet Switched Port Analyzer (SPAN) or an Encapsulated Remote Switched Port Analyzer (ERSPAN) session configuration, use the **description** command. To remove the description, use the **no** form of this command.

description *description*

no description

Syntax Description

<i>description</i>	String description of the SPAN session configuration. This string is limited to 80 characters.
--------------------	--

Command Default

No description is added.

Command Modes

SPAN session configuration mode
ERSPAN session configuration mode

Command History

Release	Modification
5.0(3)U2(2)	This command was introduced.

Usage Guidelines

The **description** command is meant to provide a reminder in the configuration to describe what certain SPAN sessions are used for. The description appears in the output of the **show monitor session** and **show running-config monitor** commands.

Examples

This example shows how to add a description for a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 9 type local
switch(config-monitor)# description A Local SPAN session
switch(config-monitor)#
```

This example shows how to add a description for an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 9 type erspan-source
switch(config-erspan-src)# description An ERSPAN session
switch(config-erspan-src)#
```

Related Commands

Command	Description
destination (SPAN session)	Configures a destination SPAN port.
monitor session	Creates a new SPAN session configuration.

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
show monitor session	Displays SPAN session configuration information.
show running-config monitor	Displays the running configuration information of a SPAN session.
source (SPAN session)	Configures a source SPAN port.

Send comments to nexus3k-docfeedback@cisco.com

destination ip (ERSPAN)

To configure an Encapsulated Remote Switched Port Analyzer (ERSPAN) destination IP address, use the **destination** command. To remove the destination ERSPAN IP address, use the **no** form of this command.

destination ip *ip_address*

no destination ip *ip_address*

Syntax Description

<i>ip_address</i>	IPv4 address in the format <i>A.B.C.D</i> .
-------------------	---

Command Default

None

Command Modes

ERSPAN source configuration mode

Command History

Release	Modification
5.0(3)U2(2)	This command was introduced.

Usage Guidelines

You can configure only one destination IP address for an ERSPAN source session.
This command does not require a license.

Examples

This example shows how to configure an ERSPAN destination IP address:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# destination ip 192.0.3.1
switch(config-erspan-src)#
```

Related Commands

Command	Description
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.
source (SPAN session)	Configures a source SPAN port.
source (ERSPAN session)	Configures a source VLAN interface.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

destination interface (ERSPAN)

To configure interfaces for an Encapsulated Remote Switched Port Analyzer (ERSPAN) destination, use the **destination interface** command. To remove the interfaces from an ERSPAN session, use the **no** form of this command.

destination interface ethernet *slot/port*

no destination interface ethernet *slot/port*

Syntax Description

ethernet	Specifies the Ethernet interface.
<i>slot/port</i>	Ethernet interface slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.

Command Default

None

Command Modes

ERSPAN destination configuration mode

Command History

Release	Modification
5.0(3)U2(2)	This command was introduced.

Usage Guidelines

The destination port should be previously configured as a switchport monitor.
This command does not require a license.

Examples

This example shows how to configure an ERSPAN destination interface:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-destination
switch(config-erspan-dst)# destination interface ethernet 1/5
switch(config-erspan-dst)#
```

Related Commands

Command	Description
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.
source (SPAN session)	Configures a source SPAN port.
source (ERSPAN session)	Configures a source VLAN interface.

Send comments to nexus3k-docfeedback@cisco.com

destination-profile (Call Home)

To create a user-defined destination profile, modify a predefined or user-defined destination profile, or configure the message format for that new destination profile, use the **destination-profile** command. To remove the destination profile, use the **no** form of this command.

```
destination-profile { CiscoTAC-1 | { { full-txt-destination | short-txt-destination } { message-level
    level | message-size size } } } { alert-group alert | email-addr email-address | http url |
    transport-method { email | http } }
```

```
destination-profile profile-name [alert-group alert | email-addr email-address | format { XML |
    full-txt | short-txt } | http url | message-level level | message-size size | transport-method
    { email | http } ]
```

```
no destination-profile
```

Syntax Description		
	CiscoTAC-1	Configures a destination profile for Extensible Markup Language (XML) messages.
	full-txt-destination	Configures a destination profile for plain text messages.
	short-txt-destination	Configures a destination profile for short text message.
	message-level <i>level</i>	Specifies the Call Home message severity level. The range is from 0 to 9, with 0 being the lowest urgency, and 9 the highest urgency.
	message-size <i>size</i>	Specifies the maximum message size. The range is as follows: <ul style="list-style-type: none"> • full-txt-destination—From 0 to 5000000, and the default is 2500000. • short-txt-destination—From 0 to 100000, and the default is 4000. • CiscoTAC-1—5000000, which is not changeable.
	alert-group <i>alert</i>	Associates one or more alert groups with a destination profile. The <i>alert</i> group can be one of the following: <ul style="list-style-type: none"> • All—All alert groups • Cisco-TAC—Cisco TAC events • Configuration—Configuration events • Diagnostic—Diagnostic events • EEM—EEM events • Environmental—Power, fan, and temperature-related events • Inventory—Inventory status events • License—Licensing events • Linecard-Hardware—Linecard-related events • Supervisor-Hardware—Supervisor-related events • Syslog-group-port—Syslog message events filed by the port manager • System—Software-related events • Test—User-generated test events
	email-addr	Specifies the e-mail address to which the alert should be sent.

Send comments to nexus3k-docfeedback@cisco.com

<i>email-address</i>	E-mail address in email address format. The address can be a maximum of 255 alphanumeric characters and cannot contain white spaces; for example, <i>personname@companyname.com</i> .
http url	Specifies the HTTP or HTTPS URL. The <i>url</i> can be a maximum of 255 alphanumeric characters and cannot contain white spaces; for example, http://site.com/services/callserv https://site2.com/serv/CALL
transport-method	Specifies the transport method for sending Call Home messages.
email	Specifies that Call Home messages be sent through e-mail.
http	Specifies that Call Home messages be sent using HTTP.
<i>profile-name</i>	User-defined profile name. The profile name can be a maximum of 31 alphanumeric characters.
format	(Optional) Specifies the Call Home message format. The default is XML.
XML	Specifies that the Call Home message format is XML.
full-txt	Specifies that the Call Home message format is plain text.
short-txt	Specifies that the Call Home message format is a short text message.

Command Default

Message format: XML.

Message size: 2500000 for full-txt-destination, 4000 for short-txt-destination, and 4000000 for XML format.

Message level: 0

Alert group: All for full-text-destination and short-text-destination profiles. The cisco-tac alert group for the CiscoTAC-1 destination profile.

Command Modes

Callhome configuration mode

Command History

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

Usage Guidelines

You can modify the following attributes for a predefined or user-defined destination profile:

- Destination e-mail address—The e-mail address to which the alert should be sent.
- Message formatting—The message format used for sending the alert (full text, short text, or XML).
- Message level—The Call Home message severity level for this destination profile.
- Message size—The allowed length of a Call Home message sent to the e-mail addresses in this destination profile.

**Note**

You cannot modify or delete the CiscoTAC-1 destination profile.

Send comments to nexus3k-docfeedback@cisco.com

The Cisco Nexus 3000 Series switch does not generate an alert if the Call Home severity level of the alert is lower than the message severity level set for the destination profile.

Table 1-1 lists each Call Home message level keyword.

Table 1-1 Call Home Message Severity Level

Call Home Level	Keyword	Description
9	Catastrophic	Network-wide catastrophic failure.
8	Disaster	Significant network impact.
7	Fatal	System is unusable.
6	Critical	Critical conditions that indicate that immediate attention is needed.
5	Major	Major conditions.
4	Minor	Minor conditions.
3	Warning	Warning conditions.
2	Notification	Basic notification and informational messages.
1	Normal	Normal event signifying return to normal state.
0	Debugging	Debugging messages.

Examples

This example shows how to create a user-defined Call Home destination profile to send Call Home messages through e-mail:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# destination-profile myProfile alert-group Configuration
email-addr myname@somecompany.com message-level 3 transport-method email
switch(config-callhome)#
```

Related Commands

Command	Description
callhome	Configures a Call Home service.
copy running-config startup-config	Saves this configuration change.
show callhome	Displays Call Home configuration information.
show callhome destination-profile	Displays Call Home information for a destination profile.

Send comments to nexus3k-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
5.0(3)U1(1)	This command was introduced.

Examples

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

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

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

```
switch# configure terminal
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 nexus3k-docfeedback@cisco.com

duplicate-message throttle (Call Home)

To limit the number of duplicate messages received for the same event, use the **duplicate-message throttle** command. To disable duplicate message throttling for Call Home, use the **no** form of this command.

duplicate-message throttle

no duplicate-message throttle

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Callhome configuration mode

Command History

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

Usage Guidelines

By default, the switch limits the number of duplicate messages received for the same event. If the number of duplicate messages sent exceeds 30 messages within a 2-hour time frame, then the switch discards further messages for that alert type.

Examples

This example shows how to enable duplicate alert message throttling for Call Home:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# duplicate-message throttle
switch(config-callhome)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves this configuration change.
show callhome	Displays Call Home configuration information.

Send comments to nexus3k-docfeedback@cisco.com

email-contact (Call Home)

To configure the e-mail address for the primary person responsible for the switch, use the **email-contact** command. To remove an email contact, use the **no** form of this command.

email-contact *email-address*

no email-contact

Syntax Description	<i>email-address</i>	E-mail address. The address can be a maximum of 255 alphanumeric characters in e-mail address format and cannot contain spaces.
--------------------	----------------------	---

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

Command Modes	Callhome configuration mode
---------------	-----------------------------

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

Examples	<p>This example shows how to configure an e-mail address:</p> <pre>switch# configure terminal switch(config)# callhome switch(config-callhome)# email-contact abc@xyz.com switch(config-callhome)#</pre>
----------	---

Related Commands	Command	Description
	copy running-config startup-config	Saves this configuration change.
	phone-contact	Configures the phone number for the primary person responsible for the switch.
	show callhome	Displays a summary of the Call Home configuration.

Send comments to nexus3k-docfeedback@cisco.com

enable (Call Home)

To enable the Cisco Smart Call Home service after you have configured the contact information, use the **enable** command. To disable the Smart Call Home service, use the **no enable** form of this command.

enable

no enable

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

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

Command Modes	Callhome configuration mode
----------------------	-----------------------------

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

Usage Guidelines	You must configure an e-mail server. Your switch must have IP connectivity to an e-mail server. You must configure the contact name (SNMP server contact), phone, and street address information before you enable Call Home.
-------------------------	---

Examples	This example shows how to enable the Cisco Smart Call Home service:
-----------------	---

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# enable
contact email address is not configured
callhome can not be enabled on the switch, because necessary configuration has not been
done
Please check if all of following configuration is done
contact person name(sysContact)
contact person's email
contact person's phone number
street addr
To configure sysContact, please use snmp-server command
switch(config-callhome)#
```

This example shows how to disable the Cisco Smart Call Home service:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# no enable
switch(config-callhome)#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	copy running-config startup-config	Saves this configuration change.
	email-contact	Configures the e-mail address.
	show callhome	Displays a summary of the Call Home configuration.

Send comments to nexus3k-docfeedback@cisco.com

event cli

To specify the event criteria for an Embedded Event Manager configuration mode(EEM) applet that is run by matching a Cisco NX-OS command-line interface (CLI) command, use the **event cli** command. To remove the CLI command event criteria, use the **no** form of this command.

event cli [*tag tag*] **match** *regex* [**count** *count-number*]

no event cli match *regex* [**count** *count-number*]

Syntax Description	tag <i>tag</i>	(Optional) Identifies this specific event when multiple events are included in the policy. The tag name can be any alphanumeric string up to 29 characters.
	match <i>regex</i>	Specifies the regular expression (regex) used to perform the CLI command pattern match. The regex can be up to 512 characters. Use * to wildcard a token.
	count <i>count-number</i>	(Optional) Specifies the number of matching occurrences before an EEM event is triggered. The <i>count-number</i> must be an integer that is greater than 0.

Defaults	None
-----------------	------

Command Modes	Embedded event manager configuration mode
----------------------	---

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

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to specify a CLI command for the EEM applet to match:
-----------------	--

```
switch# configure terminal
switch(config)# event manager applet eventcli-applet
switch(config-applet)# event cli match "shutdown" count 10
switch(config-applet)#
```

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

event counter

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a named counter crossing a threshold, use the **event counter** command. To remove the counter event criteria, use the **no** form of this command.

```
event counter name name entry-val value entry-op { eq | ge | gt | le | lt | ne } [exit-val value exit-op { eq | ge | gt | le | lt | ne }]
```

```
no event counter name name
```

Syntax Description	
name <i>name</i>	Specifies the name of the counter that will be monitored. The <i>name</i> identifier can be any alphanumeric string up to 28 characters.
entry-val <i>value</i>	Specifies the value with which the contents of the current counter are compared to decide if a counter event should be raised. The range is from 1 to 2147483647.
entry-op <i>op</i>	Compares the contents of the current counter value with the entry value using the specified operator: <ul style="list-style-type: none"> • eq—Equal to • ge—Greater than or equal to • gt—Greater than • le—Less than or equal to • lt—Less than • ne—Not equal to <p>If there is a match, an event is triggered and event monitoring is disabled until the exit criteria are met.</p>
exit-val <i>value</i>	(Optional) Specifies the value with which the contents of the current counter are compared to decide whether the exit criteria are met. The range is from 1 to 2147483647.
exit-op <i>op</i>	(Optional) Compares the contents of the current counter with the exit value using a specified operator: <ul style="list-style-type: none"> • eq—Equal to • ge—Greater than or equal to • gt—Greater than • le—Less than or equal to • lt—Less than • ne—Not equal to <p>If there is a match, an event is triggered and event monitoring is reenabled.</p>

Defaults None

Command Modes Embedded event manager configuration mode

Send comments to nexus3k-docfeedback@cisco.com

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify an event criteria for an EEM applet that is run when the defined critical_errors counter exceeds the entry value:

```
switch# configure terminal
switch(config)# event manager applet eventcntr-applet
switch(config-applet)# event counter name critical_errors entry-val 3 entry-op gt
switch(config-applet)#
```


[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

event fanabsent

To specify an event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a fan absent event, use the **event fanabsent** command. To remove the fan absent event criteria, use the **no** form of this command.

event fanabsent [*fan number*] *time interval*

no event fanabsent [*fan number*] *time interval*

Syntax Description	fan number	(Optional) Specifies a fan number to monitor for a fan absent event. The range is from 1 to 1.
	time interval	Specifies the time interval in seconds within which the fan can stay absent. The range is from 10 to 64000.

Defaults	None
-----------------	------

Command Modes	Embedded event manager configuration mode
----------------------	---

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

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to specify that an EEM applet runs when a fan absent event occurs:
-----------------	---

```
switch# configure terminal
switch(config)# event manager applet absent-applet
switch(config-applet)# event fanabsent time 600
switch(config-applet)#
```

Send comments to nexus3k-docfeedback@cisco.com

event fanbad

To specify an event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a fan bad event, use the **event fanbad** command. To remove the fan bad event criteria, use the **no** form of this command.

event fanbad *fan number* *time interval*

no event fanbad [*fan number*] *time interval*

Syntax Description	fan number	Specifies a fan number to monitor for a fan bad event. The range is from 1 to 1.
	time interval	Specifies the time interval (in seconds) within which the fan can stay bad. The range is from 10 to 64000.

Defaults	None
-----------------	------

Command Modes	Embedded event manager configuration mode
----------------------	---

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

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to specify that an EEM applet runs when a fan bad event occurs:
-----------------	--

```
switch# configure terminal
switch(config)# event manager applet bad-applet
switch(config-applet)# event fanbad time 1200
switch(config-applet)#
```

Send comments to nexus3k-docfeedback@cisco.com

event manager applet

To register an applet with the Embedded Event Manager (EEM) and enter the applet configuration mode, use the **event manager applet** command. To remove the applet configuration, use the **no** form of this command.

event manager applet *applet-name*

no event manager applet *applet-name*

Syntax Description

<i>applet-name</i>	Name of the applet. The applet name can be any case-sensitive, alphanumeric string up to 29 characters. The applet name cannot have an underscore in the first two characters.
--------------------	--

Defaults

None

Command Modes

Applet configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to register an applet and enter the applet configuration mode:

```
switch# configure terminal
switch(config)# event manager applet monitorShutdown
switch(config-applet)#
```

This example shows how to remove the applet configuration:

```
switch(config-applet)# no event manager applet monitorShutdown
switch(config-applet)#
```

Related Commands

Command	Description
description	Configures a descriptive string for the policy.
event	Configures the event statement for the policy.
show event-manager policy state	Correlates multiple events in the policy.
tag	Displays information about the status of the configured policy.

Send comments to nexus3k-docfeedback@cisco.com

event manager environment

To configure an environment variable for Embedded Event Manager (EEM), use the **event manager environment** command. To remove the environment variable, use the **no** form of this command.

event manager environment *variable-name variable-value*

no event manager environment *variable-name variable-value*

Syntax Description

<i>variable-name</i>	Name of the environment variable. The variable name can be any alphanumeric string up to 29 characters.
<i>variable-value</i>	Value of the environment. The variable value can be any case-sensitive, alphanumeric string up to 39 characters specified within quotes.

Defaults

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure an event manager variable for EEM:

```
switch# configure terminal
switch(config)# event manager environment emailto "admin@abc.com"
switch(config)#
```

This example shows how to remove the event manager variable:

```
switch(config)# no event manager environment emailto "admin@abc.com"
switch(config)#
```

Related Commands

Command	Description
show event manager environment	Displays information about the configured environment variables.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

event manager policy

To register and activate an Embedded Event Manager (EEM) script policy, use the **event manager policy** command. To remove the event manager policy, use the **no** form of this command.

event manager policy *policy-script-file*

no event track event manager policy *script-policy-file*

Syntax Description	<i>policy-script-file</i> Name of the script policy file. The policy scriptfile name can be any case-sensitive, alphanumeric string up to 29 characters.	
Defaults	None	
Command Modes	Global configuration mode	
Command History	Release	Modification
	5.0(3)U3(1)	This command was introduced.
Usage Guidelines	<p>Before using the event manager policy command, define a policy by using the virtual shell (VSH) script and copy the file to the system directory. For information on how to define a policy, see the <i>Cisco Nexus 3000 Series NX-OS System Management Configuration Guide</i>.</p> <p>This command does not require a license.</p>	
Examples	<p>This example shows how to register and activate an EEM script policy:</p> <pre>switch# configure terminal switch(config)# event manager policy modulescript switch(config)#</pre>	

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

event manager policy internal

To register and activate an Embedded Event Manager (EEM) script policy, use the **event manager policy internal** command. To remove the internal event manager policy, use the **no** form of this command.

event manager policy internal *policy-name*

no event manager policy internal *policy-name*

Syntax Description	<i>policy-name</i>	Name of the internal policy. The policy name can be any case-sensitive alphanumeric string up to 29 characters.
--------------------	--------------------	---

Defaults	None
----------	------

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

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

Usage Guidelines	Before using the event manager policy internal command, define a policy by using the virtual shell (VSH) script and copy the file to the system directory. For information on how to define a policy, see the <i>Cisco Nexus 3000 Series NX-OS System Management Configuration Guide</i> .
------------------	---

This command does not require a license.

Examples	This example shows how to register and activate an EEM internal policy:
----------	---

```
switch# configure terminal
switch(config)# event manager policy internal modulescript
switch(config)#
```

Send comments to nexus3k-docfeedback@cisco.com

event memory

To specify an event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a memory threshold, use the **event memory** command. To remove the memory event criteria, use the **no** form of this command.

event memory [critical | minor | severe]

no event memory [critical | minor | severe]

Syntax Description

critical	Specifies a critical alert.
minor	Specifies a minor alert.
severe	Specifies a severe alert.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify that an EEM applet runs when a memory threshold is exceeded:

```
switch# configure terminal
switch(config) event manager applet cli-event
switch(config-applet)# event memory critical
switch(config-applet)#
```

Send comments to nexus3k-docfeedback@cisco.com

event oir

To specify an event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of an Online-Insertion-Removal (OIR), use the **event oir** command. To remove the OIR event criteria, use the **no** form of this command.

```
event oir { fan [anyoir | insert | remove] | module [anyoir | insert | remove] | powersupply [anyoir
| insert | remove] | tag tag }
```

```
no event oir { fan [anyoir | insert | remove] | module [anyoir | insert | remove] | powersupply
[anyoir | insert | remove] | tag tag }
```

Syntax Description

fan	Specifies a fan OIR event.
anyoir	(Optional) Specifies any OIR event.
insert	(Optional) Specifies the OIR insert event.
remove	(Optional) Specifies the OIR remove event.
module	Specifies the module OIR event.
powersupply	Specifies a power supply OIR event.
tag tag	Identifies this specific event when multiple events are included in the policy. The tag name can be any alphanumeric string up to 29 characters.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify that an EEM applet runs when an OIR occurs:

```
switch# configure terminal
switch(config) event manager applet cli-event
switch(config-applet)# event oir fan remove 1
switch(config-applet)#
```


Send comments to nexus3k-docfeedback@cisco.com

event policy-default

To configure an event in case a system policy is being overridden, use the **event policy-default** command. To use the overridden policy, use the **no** form of this command.

event policy-default count *count* **time** *seconds*

no event policy-default count *count* **time** *seconds*

Syntax Description	count <i>count</i>	Specifies the number of matching occurrences before a default event is triggered. The range is from 1 to 65000.
	time <i>seconds</i>	Specifies the interval in seconds, within which the events need to happen. The range is from 0 to 4294967295.

Defaults	None
-----------------	------

Command Modes	Embedded event manager configuration mode
----------------------	---

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

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to configure an event in case a system policy is being overridden:
	<pre>switch# configure terminal switch(config) event manager applet cli-event switch(config-applet)# event policy-default count 15 time 1500 switch(config-applet)#</pre>

Send comments to nexus3k-docfeedback@cisco.com

event snmp

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run by sampling Simple Network Management Protocol (SNMP) object identifier (OID) values, use the **event snmp** command. To remove the SNMP event criteria, use the **no** form of this command.

```
event snmp [tag tag] oid value get-type {exact | next} entry-op {gt | ge | eq | ne | lt | le} entry-val
value [{exit-comb {or | and} exit-op {gt | ge | eq | ne | lt | le} exit-val value exit-time time} |
{exit-op {gt | ge | eq | ne | lt | le} exit-val value}] poll-interval value
```

```
no event snmp [tag tag] oid value get-type {exact | next} entry-op {gt | ge | eq | ne | lt | le}
entry-val value [{exit-comb {or | and} exit-op {gt | ge | eq | ne | lt | le} exit-val value exit-time
time} | {exit-op {gt | ge | eq | ne | lt | le} exit-val value}] poll-interval value
```

Syntax Description

tag <i>tag</i>	(Optional) Identifies this specific event when multiple events are included in the policy. The tag name can be any alphanumeric string up to 29 characters.
oid <i>value</i>	Specifies the SNMP OID values in the <i>value</i> argument as the event criteria. The <i>value</i> of the data element must be in SNMP dotted notation. An OID is defined as a type in the associated MIB and each type has an object value. Monitoring of some OID types is supported. When the oid keyword is used, an error message is returned if the OID is not one of the following: <ul style="list-style-type: none"> • INTEGER_TYPE • COUNTER_TYPE • GAUGE_TYPE • TIME_TICKS_TYPE • COUNTER_64_TYPE • OCTET_PRIM_TYPE • OPAQUE_PRIM_TYPE
get-type	Specifies the type of SNMP get operation to be applied to the object ID specified by the oid <i>value</i> argument.
exact	Retrieves the object ID specified by the oid <i>value</i> argument.
next	Retrieves the object ID that is the alphanumeric successor to the object ID specified by the oid <i>value</i> argument.
entry-op <i>op</i>	Compares the contents of the current object ID value with the entry value using the specified operator: <ul style="list-style-type: none"> • gt—Greater than • ge—Greater than or equal to • eq—Equal to • ne—Not equal to • lt—Less than • le—Less than or equal to <p>If there is a match, an event is triggered and event monitoring is disabled until the exit criteria are met.</p>

Send comments to nexus3k-docfeedback@cisco.com

entry-val <i>value</i>	Specifies the <i>value</i> with which the contents of the current object ID are compared to decide if an SNMP event should be raised. The range is from 0 to 18446744073709551615.
exit-comb	(Optional) Indicates the combination of exit conditions that must be met before event monitoring is reenabled.
or	(Optional) Specifies that an exit comparison operator and an exit object ID value or an exit time value must exist.
and	(Optional) Specifies that an exit comparison operator, an exit object ID value, and an exit time value must exist.
exit-op <i>op</i>	<p>(Optional) Compares the contents of the current object ID with the exit value using the specified operator:</p> <ul style="list-style-type: none"> • gt—Greater than • ge—Greater than or equal to • eq—Equal to • ne—Not equal to • lt—Less than • le—Less than or equal to <p>If there is a match, an event is triggered and event monitoring is reenabled.</p> <p>Note This keyword and its argument are not optional if the exit-comb keyword is defined.</p>
exit-val <i>value</i>	<p>(Optional) Specifies the value with which the contents of the current object ID are compared to decide whether the exit criteria are met. The range is from 0 to 18446744073709551615.</p> <p>Note This keyword and its argument are not optional if the exit-comb keyword is defined.</p>
poll-interval <i>value</i>	Specifies the time interval between consecutive polls. The <i>value</i> is an integer that represents seconds in the range from 1 to 2147483647.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Send comments to nexus3k-docfeedback@cisco.com

Examples

This example shows how to specify the event criteria for an EEM applet that is run by sampling SNMP object identifier values:

```
switch# configure terminal
switch(config)# event manager applet snmp-applet
switch(config-applet)# event snmp oid 4.2.1.6 get-type next entry-op eq entry-val 42
poll-interval 30000
switch(config-applet)#
```

Send comments to nexus3k-docfeedback@cisco.com

event storm-control

To specify an event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a storm-control, use the **event storm-control** command. To remove the storm-control event criteria, use the **no** form of this command.

event storm-control

no event storm-control

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

Defaults	None
-----------------	------

Command Modes	Embedded event manager configuration mode
----------------------	---

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

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to specify that an EEM applet runs when a storm-control occurs:
-----------------	--

```
switch# configure terminal
switch(config) event manager applet cli-event
switch(config-applet)# event storm-control
switch(config-applet)#
```

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

event syslog

To specify an event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a syslog, use the **event syslog** command. To remove the syslog event criteria, use the **no** form of this command.

event syslog [*occurs occurs* | **pattern** *pattern* | **period** *period* | **priority** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **pattern** *pattern* | **warnings**} **pattern** | **tag**]

no event syslog [*occurs occurs* | **pattern** *pattern* | **period** *period* | **priority** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **pattern** *pattern* | **warnings**} **pattern** | **tag**]

Syntax Description

occurs <i>occurs</i>	Specifies an integer to be used for number of occurrences. The range is from 1 to 65000.
pattern <i>pattern</i>	Specifies a regular expression to be used for matching. The pattern can be any alphanumeric string up to 256 characters.
period <i>period</i>	Specifies the time interval within which the events need to happen. The range is from 0 to 4294967295.
priority	Specifies the priority of the log message.
alerts	Specifies the alert log message.
critical	Specifies the critical log message.
debugging	Specifies the debugging log message.
emergencies	Specifies the emergency log message.
errors	Specifies the error log message.
informational	Specifies the informational log message.
notifications	Specifies the notifications log message.
warnings	Specifies the warning log message.
tag	Identifies this specific event when multiple events are included in the policy.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Send comments to nexus3k-docfeedback@cisco.com

Examples

This example shows how to specify that an EEM applet runs when a syslog message is matched:

```
switch# configure terminal
switch(config) event manager applet cli-event
switch(config-applet)# event syslog period 120 pattern "interface ethernet 1/3 state down"
Configuration accepted successfully
switch(config-applet)#
```

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

event sysmgr

To specify an event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of the system manager event, use the **event sysmgr** command. To remove the system manager event criteria, use the **no** form of this command.

event sysmgr [**memory** [**major** *major-percent* **minor** *minor-percent* **clear** *clear-percent* | **module** *module-number*] | **switchover** **count** *count* **time** *time-interval*]

no event sysmgr

Syntax Description		
memory	(Optional)	Specifies the memory alert event.
major <i>major-percent</i>	(Optional)	Sets the major memory threshold. The range is from 1 to 99.
minor <i>minor-percent</i>	(Optional)	Sets the minor memory threshold. The range is from 1 to 99.
clear <i>clear-percent</i>	(Optional)	Sets the percentage of memory that needs to be cleared. The range is from 1 to 99.
module <i>module-number</i>	(Optional)	Specifies the module number. The module number range is from 1 to 1.
switchover	(Optional)	Specifies the switchover-related events.
count <i>count</i>	(Optional)	Specifies the number of switchovers after which the event should be triggered. The range is from 1 to 65000.
time <i>time-interval</i>	(Optional)	Specifies the time interval within which the events need to happen. The range is from 1 to 4294967295.

Defaults None

Command Modes Embedded event manager configuration mode

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

Usage Guidelines This command does not require a license.

Send comments to nexus3k-docfeedback@cisco.com

Examples

This example shows how to specify that an EEM applet runs when a syslog message is matched:

```
switch# configure terminal
switch(config) event manager applet cli-event
switch(config-applet)# event sysmgr memory major 34 minor 76 clear 10
Configuration error. memroy threshold policy has to override the default syste
policy of __sysmgr_policy_mem_alert.
switch(config-applet)#switch(config-applet)#
```

Send comments to nexus3k-docfeedback@cisco.com

event temperature

To specify an event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a temperature event, use the **event temperature** command. To remove the temperature event criteria, use the **no event temperature** form of this command.

event temperature [*module module*] [*sensor number*] **threshold** {**any** | **major** | **minor**}

no event temperature [*module module*] [*sensor number*] **threshold** {**any** | **major** | **minor**}

Syntax Description

module <i>module</i>	(Optional) Specifies that a specific module must be monitored. The range is from 1 to 1.
sensor <i>number</i>	(Optional) Specify that a specific sensor must be monitored. The range is from 1 to 8.
threshold	Specifies the threshold event that triggers the EEM applet. Choose either major , minor , or any .
any	Specifies any event.
major	Specifies a major event.
minor	Specifies a minor event.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify that an EEM applet runs when a temperature event occurs:

```
switch# configure terminal
switch(config)# event manager applet temp-applet
switch(config-applet)# event temperature threshold major
switch(config-applet)#
```

Send comments to nexus3k-docfeedback@cisco.com

event track

To specify the event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of an object tracking subsystem report for the specified object number, use the **event track** command. To remove the report event criteria, use the **no** form of this command.

event track [**tag** *tag*] *object-id* **state** {**any** | **up** | **down**}

no event track [**tag** *tag*] *object-id*

Syntax Description

tag <i>tag</i>	(Optional) Identifies this specific event when multiple events are included in the policy.
<i>object-id</i>	Tracked object number. The range from 1 to 500.
state	Specifies that the tracked object transition causes an event to be raised.
any	Specifies an event is to be raised when the tracked object transitions to or from any state.
up	Specifies an event is to be raised when the tracked object transitions from a down state to an up state.
down	Specifies an event is to be raised when the tracked object transitions from an up state to a down state.

Defaults

None

Command Modes

Embedded event manager configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify that an EEM applet runs when the state of a tracked object changes:

```
switch# configure terminal
switch(config)# event manager applet tracking-applet
switch(config-applet)# event track 20 state down
switch(config-applet)#
```

Send comments to nexus3k-docfeedback@cisco.com

feature ntp

To enable the Network Time Protocol (NTP), use the **feature ntp** command. To disable NTP, use the **no** form of this command.

feature ntp

no feature ntp

Syntax Description

This command does not have any arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable NTP:

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

This example shows how to disable NTP:

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

Related Commands

Command	Description
ntp master	Configures the device to act as an authoritative NTP server.

Send comments to nexus3k-docfeedback@cisco.com

feature ptp

To enable the Precision Time Protocol (PTP) feature, use the **feature ptp** command. To disable the PTP feature, use the **no** form of this command.

feature ptp

no feature ptp

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

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

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

SupportedUserRoles	network-admin vdc-admin
---------------------------	----------------------------

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

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to enable the PTP feature:
-----------------	---

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

This example shows how to disable the PTP feature:

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

Related Commands	Command	Description
	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.
	ptp priority2	Configures the priority2 value to use when advertising this clock.

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.

Send comments to nexus3k-docfeedback@cisco.com

feature scheduler

To enable the scheduler feature on a Cisco NX-OS device, use the **feature scheduler** command. To disable the schedule feature, use the **no** form of this command.

feature scheduler

no feature scheduler

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

Defaults	Disabled
-----------------	----------

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

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

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to enable the scheduler feature on a Cisco NX-OS device:
-----------------	---

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

This example shows how to disable the scheduler feature on a Cisco NX-OS device:

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

Related Commands	Command	Description
	scheduler	Configures maintenance jobs.

Send comments to nexus3k-docfeedback@cisco.com

feature sflow

To enable the scheduler feature on a Cisco NX-OS device, use the **feature sflow** command. To disable the schedule feature, use the **no** form of this command.

feature sflow

no feature sflow

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

Defaults	Disabled
-----------------	----------

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

Command History	Release	Modification
	5.0(3)U4(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to enable the sFlow feature on a Cisco NX-OS device:
-----------------	---

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

This example shows how to disable the sFlow feature on a Cisco NX-OS device:

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

Related Commands	Command	Description
	sflow sampling-rate	.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

filter access-group

To configure the SPAN source sessions so that ingress (RX) traffic is filtered by using ACLS, use the **filter access-group** command.

filter access-group *acl-name*

Syntax Description	<i>acl-name</i> Name of the Access Control List.
--------------------	--

Defaults	None.
----------	-------

Command Modes	Monitor configuration mode.
---------------	-----------------------------

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

Usage Guidelines	This command filters only ingress traffic for SPAN and ERSPAN source ports based on an IP access-list, not an access-map.
------------------	---

Examples	This example shows how to filter ingress traffic at a SPAN source port:
----------	---

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# filter access-group acl1
switch(config-monitor)# source interface ethernet 1/16
```

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

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# filter access-group acl1
switch(config-monitor)# source interface port-channel 1 rx
```

This example shows how to configure a VLAN SPAN source with ACL filtering:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# filter access-group acl1
switch(config-monitor)# source vlan 1
```

Related Commands	Command	Description
	show monitor session	Displays SPAN session configuration information.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

hardware profile buffer info port-threshold

To configure the port buffer information threshold so that a syslog message is generated when the buffer capacity reaches the specified percentage, use the **hardware profile buffer info port-threshold** command. The **no** form of this command is not supported.

hardware profile buffer info port-threshold *front-port port-number threshold percentage*

Syntax Description	front-port	Specifies to configure a front port.
	<i>port-number</i>	Number of the port. The range is from 1 to 64.
	threshold	Specifies to configure the threshold.
	<i>percentage</i>	Percentage of buffer capacity. The range is from 1 to 95. The default value is 90 percent.

Defaults The port buffer information threshold is 90 percent.

Command Modes Global configuration mode

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

Usage Guidelines This command does not require a license.

Examples This example shows how to set the port buffer information threshold to 80 percent for port 1:

```
switch# configure terminal
switch(config)# hardware profile buffer info port-threshold front-port 1 threshold 80
switch(config)#
```

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

Send comments to nexus3k-docfeedback@cisco.com

hardware profile parity-error

To clear a corresponding table entry (with 0s) when a parity error is detected, use the **hardware profile parity-error** command. To disable this feature, use the **no** form of this command.

hardware profile parity-error {l2-table | l3-table} clear

no hardware profile parity-error {l2-table | l3-table} clear

Syntax	l2-table clear	Specifies to clear parity error entries in a Layer 2 table.
	l3-table clear	Specifies to clear parity error entries in a Layer 3 table.

Command Default None

Command Modes Global configuration mode

Command History	Release	Modification
	6.0(2)U2(1)	This command was dropped.
	5.0(3)U5(1a)	This command was introduced.

Usage Guidelines The following guidelines apply:

- When the command is used for an l2_entry table, the cleared entry should be relearned due to the traffic pattern.
- When the command is used for an l3_entry_only (host) table, the cleared entry is not be relearned.

The command is useful in the following customer configurations:

- L2_Entry table, with no static L2_entry table entries

If the L2_Entry table entry is cleared, the entry should be dynamically learned through the traffic pattern. It should not be learned through IGMP or multicast.

- L3_Entry_only (host) table

Customers should not use the host table. The hardware profile unicast enable-host-ecmp command should be enabled. In this case, the customer node does not have any valid entries in the L3_Entry_only table, so clearing the L3_Entry_only entry table should not have any impact.

This command is effective when it is present in the running configuration and the system is booting up. In addition, the command must be enabled and after the configuration is saved, the system should be rebooted for the command to take effect.

Examples This example shows how to clear parity errors in a Layer 2 table:

```
switch# configure terminal
```

Send comments to nexus3k-docfeedback@cisco.com

```
switch(config)# hardware profile parity-error l2-table clear
switch(config)# copy running-config startup-config
switch(config)# reload
```

This example shows how to clear parity errors in a Layer 3 table:

```
switch# configure terminal
switch(config)# hardware profile parity-error l3-table clear
switch(config)# copy running-config startup-config
switch(config)# reload
```

Related Commands

Command	Description
reload	Reloads the Cisco Nexus 3000 Series switch software.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

hardware profile tap-aggregation

Command	Description
reload	Reloads the Cisco Nexus 3000 Series switch software.

To enable the tap aggregation feature and reserve entries in the interface table that are needed for VLAN tagging, use the **hardware profile tap-aggregation** command. To disable this feature, use the **no** form of this command.

hardware profile tap-aggregation [l2drop]

no hardware profile tap-aggregation [l2drop]

Syntax Description	l2drop	Specifies to drop non IP traffic ingress on mode tap interfaces.
---------------------------	---------------	--

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

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

Command History	Release	Modification
	6.0(2)U3(1)	The l2drop option was added.
	6.0(2)U2(3)	This command was introduced.

Usage Guidelines	<p>You can use this command on all Cisco Nexus 3000 Series and Cisco Nexus 3100 Series switches.</p> <p>Ensure that you run the copy running-config to startup-config command to save the configuration to startup, and reload the switch to enable tap-aggregation.</p>
-------------------------	---

Examples	This example shows how to configure Tap Aggregation globally on the switch:
-----------------	---

```
switch# configure terminal
switch(config)# hardware profile tap-aggregation
switch(config)# copy running-config startup-config
switch(config)# reload
```

Related Commands	Command	Description
	reload	Reloads the Cisco Nexus 3000 Series switch software.

Send comments to nexus3k-docfeedback@cisco.com

hardware profile unicast syslog host-table-detail

When an IPv4 host table is full and the prefixes are programmed in LPM, the following syslog message is displayed:

```
$ %IPFIB-2-FIB_TCAM_RESOURCE_EXHAUSTION_HOST_IPV4: FIB TCAM exhausted for IPV4 routes in Host table, IPV4 Host routes will be programmed in LPM table if possible.
```

With the introduction of the ALPM Mode (**system routing max-mode l3**) on the Cisco Nexus 3100 series switches, an additional syslog is introduced (one of the two, depending on whether the ALPM mode is enabled or not). The following syslogs are for IPv4. IPv6 has a similar syslog message.

- When the ALPM Mode is not enabled, the following syslog message is displayed:

```
$ IPFIB-2-FIB_TCAM_RESOURCE_EXHAUSTION_HOST_IPV4_ENABLE_ALPM: FIB TCAM exhausted for IPV4 routes in Host table, IPV4 Host routes will be programmed in LPM table if possible. Consider enabling ALPM mode
```
- When the ALPM Mode is enabled, the following syslog message is displayed:

```
$ %IPFIB-2-FIB_TCAM_RESOURCE_EXHAUSTION_HOST_IPV4_LPM_TABLE: FIB TCAM exhausted for IPV4 routes in Host table, IPV4 Host routes will be programmed in LPM table if possible. Check 'show hardware profile status' for table utilization.
```

To prevent confusion between the two syslog messages, a new CLI has been added to suppress the first log. Use the **[no] hardware profile unicast syslog host-table-detail** command to suppress the syslog.

```
hardware profile unicast syslog host-table-detail
[no] hardware profile unicast syslog host-table-detail
```

Syntax Description	host-table-detail Specifies the details of the entries in the host table.
--------------------	--

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

Command History	Release	Modification
	6.0(2)U5(4)	This command was introduced.

Usage Guidelines	This command does not require a license.
------------------	--

Examples

This example shows how to suppress the existing syslog when the IPv4 or IPv6 table is full:

switch# **configure terminal**
switch(config)# **hardware profile unicast syslog host-table-detail**
\$ %IPFIB-2-FIB_TCAM_RESOURCE_EXHAUSTION_HOST_IPV4: FIB TCAM exhausted for IPV4 routes in Host table, IPV4 Host routes will be programmed in LPM table if possible.

Send comments to nexus3k-docfeedback@cisco.com

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

Send comments to nexus3k-docfeedback@cisco.com

ip access-list (session)

Command	Description
reload	Reloads the Cisco Nexus 3000 Series switch software.

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

Examples

This example shows how to create an IPv4 ACL for a configuration session:

```
switch# configure session MySession1
switch(config-s)# ip access-list myACL
switch(config-s-acl)#
```

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 nexus3k-docfeedback@cisco.com](mailto:nexus3k-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	<i>domain-name</i>	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)U1(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# configure terminal
switch(config)# ip domain-list Mysite.com
switch(config)#
```

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

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

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

Send comments to nexus3k-docfeedback@cisco.com

```
switch(config)# ip name-server 192.0.2.1
switch(config)# ip domain-list Mysite2.com
switch(config)#
```

Related Commands

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

Send comments to nexus3k-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)U1(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# configure 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 nexus3k-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)U1(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 name for a particular VRF.
-------------------------	--

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

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

Send comments to nexus3k-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 nexus3k-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</i> ... <i>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)U1(1)	This command was introduced.

Usage Guidelines

Use the **ip host** command to add a static host name to DNS.

Examples

This example shows how to configure a static hostname:

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

Related Commands

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

Send comments to nexus3k-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)U1(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# configure 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)#
```

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

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

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# configure terminal
switch(config)# vrf context management
switch(config-vrf)# exit
```

Send comments to nexus3k-docfeedback@cisco.com

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

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 nexus3k-docfeedback@cisco.com](mailto:nexus3k-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.
	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
	5.0(3)U1(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 nexus3k-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
	5.0(3)U1(1)	This command was introduced.

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

```
switch# configure terminal
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 nexus3k-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
	5.0(3)U1(1)	This command was introduced.

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

```
switch# configure terminal
switch(config)# logging distribute
switch(config)# logging 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 nexus3k-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** form of this command.

logging console [*severity-level*]

no logging console

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

Examples

This example shows how to enable logging messages with a severity level of 4 (warning) or higher to the console session:

```
switch# configure terminal
switch(config)# logging console 4
switch(config)#
```

Related Commands

Command	Description
show logging console	Displays the console logging configuration.

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

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

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

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

```
switch# configure terminal
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 nexus3k-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 {link-status | trunk-status} {default | enable}

no logging event {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
Switch profile configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U2(1)	Support to log interface events was added in switch profiles.

Examples

This example shows how to log interface events:

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

This example shows how to log TRUNK interface events in a switch profile:

```
switch# configure sync
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-sync)# switch-profile s5010
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# logging event trunk-status default
switch(config-sync-sp)#
```

Related Commands

Command	Description
show logging	Displays the logging status.
show switch-profile	Displays information about the switch profile and the configuration revision.
switch-profile	Creates or configures a switch profile.

Send comments to nexus3k-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
5.0(3)U1(1)	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
switch(config-if)#
```

Related Commands

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

Send comments to nexus3k-docfeedback@cisco.com

logging ip access-list cache entries num_entries

Sets the maximum number of log entries cached in software. The range is from 0 to 1000000 entries. The default value is 8000 entries.

logging ip access-list cache entries <num_entries>

Syntax Description	num_entries	Specifies the number of log entries.
Command Default	None	
Command Modes	Interface configuration mode	
Command History	Release	Modification
	5.0(3)U1(1)	This command was introduced.
Examples	<p>This example shows how to log interface events:</p> <pre>switch# configure terminal switch(config)# logging ip access-list cache entries 5000 switch(config)#</pre>	
Related Commands	Command	Description
	show logging	Displays the logging status.

Send comments to nexus3k-docfeedback@cisco.com

logging ip access-list cache interval seconds

Sets the number of seconds between log updates. Also if an entry is inactive for this duration, it is removed from the cache. The range is from 5 to 86400 seconds. The default value is 300 seconds.

logging ip access-list cache interval <seconds>

Syntax Description	interval	The number of seconds between log updates.
Command Default	None	
Command Modes	Interface configuration mode	
Command History	Release	Modification
	5.0(3)U1(1)	This command was introduced.
Examples	<p>This example shows how to log interface events:</p> <pre>switch# configure terminal switch(config)# logging ip access-list cache interval 120 switch(config)#</pre>	
Related Commands	Command	Description
	show logging	Displays the logging status.

Send comments to nexus3k-docfeedback@cisco.com

logging ip access-list cache threshold num_packets

Sets the number of packet matches before an entry is logged. The range is from 0 to 1000000 packets. The default value is 0 packets, which means that logging is not triggered by the number of packet matches.

logging ip access-list cache threshold <num_packets>

Syntax Description	num_packets	The number of packet matches before an entry is logged.
Command Default	None	
Command Modes	Interface configuration mode	
Command History	Release	Modification
	5.0(3)U1(1)	This command was introduced.
Examples	<p>This example shows how to log interface events:</p> <pre>switch# configure terminal switch(config)# logging ip access-list cache threshold 500000 switch(config)#</pre>	
Related Commands	Command	Description
	show logging	Displays the logging status.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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. 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
	5.0(3)U1(1)	This command was introduced.

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

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

This example shows how to enable error logging messages for the Precision Time Protocol (PTP) packets:

```
switch# configure terminal
switch(config)# logging level ptp 3
```

Send comments to nexus3k-docfeedback@cisco.com

```
switch(config)#
```

Related Commands

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
	5.0(3)U1(1)	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# configure terminal
switch(config)# logging logfile logfile 4
switch(config)#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands

Command	Description
show logging logfile	Displays the log file.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.0(3)U1(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	5.0(3)U1(1)	This command was introduced.
Release	Modification				
5.0(3)U1(1)	This command was introduced.				
Usage Guidelines	Set a specified severity level or use the default.				
Examples	<p>This example shows how to enable module log messages:</p> <pre>switch# configure terminal switch(config)# logging module switch(config)#</pre>				
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show logging module</td><td>Displays the module logging status.</td></tr></table>	Command	Description	show logging module	Displays the module logging status.
Command	Description				
show logging module	Displays the module logging status.				

Send comments to nexus3k-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
5.0(3)U1(1)	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# configure terminal
switch(config)# logging monitor
switch(config)#
```

Related Commands

Command	Description
show logging monitor	Displays the status of monitor logging.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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** *facility* | **use-vrf** {*vrf_name* | **management**}]

no logging server *host* [*severity-level*] [**facility** *facility* | **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 facility can be one of the following: auth , authpriv , cron , daemon , ftp , kernel , local0 , local1 , local2 , local3 , local4 , local5 , local6 , local7 , lpr , mail , news , syslog , user , uucp 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
	5.0(3)U1(1)	This command was introduced.

Send comments to nexus3k-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# configure terminal
switch(config)# logging server 192.168.2.253
switch(config)#
```

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

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

Related Commands

Command	Description
show logging server	Displays the configured syslog servers.

Send comments to nexus3k-docfeedback@cisco.com

logging source-interface

To enable a source interface for the remote syslog server, use the **logging source-interface** command. To disable the source interface, use the **no** form of this command.

logging source-interface [**ethernet** *slot/port* | **loopback** *interface-number* | **mgmt** *interface-number* | **port-channel** *port-channel-number* | **vlan** *interface-number* | **tunnel** *interface-number*]

no logging source-interface [**ethernet** *slot/port* | **loopback** *interface-number* | **mgmt** *interface-number* | **port-channel** *port-channel-number* | **vlan** *interface-number* | **tunnel** *interface-number*]

Syntax Description		
ethernet <i>slot/port</i>		Specifies Ethernet as the source interface. The range for the Ethernet option is from 1 to 253.
loopback <i>interface-number</i>		Specifies loopback as the source interface. The range for the loopback option is from 1 to 1023.
mgmt <i>interface-number</i>		Specifies management as the source interface. The interface number management option is 0.
port-channel <i>port-channel-number</i>		Specifies port-channel as the source interface. The range for the port-channel option is from 1 to 4096.
vlan <i>interface-number</i>		Specifies VLAN as the source interface.
tunnel <i>interface-number</i>		Specifies tunnel as the source interface.

Command Default None.

Command Modes Global configuration mode

Command History	Release	Modification
	5.0(3)U5(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to enable a source interface for the syslog server:

```
switch# configure terminal
switch(config)# logging source-interface ethernet 2/1
```

Related Commands	Command	Description
	show logging info	Displays the configured syslog information.

Send comments to nexus3k-docfeedback@cisco.com

Send comments to nexus3k-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
	5.0(3)U1(1)	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:	
	<pre>switch# configure terminal switch(config)# logging timestamp microseconds switch(config)#</pre>	
Related Commands	Command	Description
	show logging timestamp	Displays the logging time-stamp configuration.

Send comments to nexus3k-docfeedback@cisco.com

mode tap-aggregation

To allow the attachment of an ACL with a Tap Aggregation policy to an interface, use the **mode tap-aggregation** command. To disallow the attachment of such a policy to an interface, use the **no** form of this command.

mode tap-aggregation

no mode tap-aggregation

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

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

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

Command History	Release	Modification
	6.0(2)U2(3)	This command was introduced.

Usage Guidelines	<p>You can use this command on all Cisco Nexus 3000 Series and Cisco Nexus 3100 Series switches.</p> <p>To be able to apply an ACL with a Tap Aggregation policy on an interface, you must run the mode tap-aggregation command.</p>
-------------------------	---

Examples	This example shows how to enable mode tap-aggregation and apply the ACL on an interface:
-----------------	--

```
switch# configure terminal
switch(config)# interface ethernet1/2
switch(config-if)# mode tap-aggregation
switch(config-if)# ip port access-group test in
```

Related Commands	Command	Description
	ip port access-group	Applies an ACL to an interface.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

monitor erspan origin ip-address

To configure the Encapsulated Remote Switched Port Analyzer (ERSPAN) global origin IP address, use the **monitor erspan origin ip-address** command. To remove the ERSPAN global origin IP address configuration, use the **no** form of this command.

monitor erspan origin ip-address *ip-address* [**global**]

no monitor erspan origin ip-address *ip-address* [**global**]

Syntax Description	<i>ip-address</i>	IP address.
	global	(Optional) Specifies the default global configuration.

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

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

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines	When you change the origin IP address, it impacts all the sessions.
------------------	---



Note

On a Cisco Nexus 3000 Series switch, only global origin IP address is supported.

This command does not require a license.

Examples	This example shows how to configure the ERSPAN global origin IP address:
----------	--

```
switch# configure terminal
switch(config)# monitor erspan origin ip-address 10.1.1.1 global
switch(config)#
```

This example shows how to remove the ERSPAN global origin IP address:

```
switch# configure terminal
switch(config)# no monitor erspan origin ip-address 10.1.1.1 global
switch(config)#
```

Related Commands	Command	Description
	monitor session	Configures a SPAN or an ERSPAN session.

Send comments to nexus3k-docfeedback@cisco.com

monitor session

To create a new Switched Port Analyzer (SPAN) or an Encapsulated Remote Switched Port Analyzer (ERSPAN) session configuration for analyzing traffic between ports, or add to an existing session configuration, use the **monitor session** command. To clear SPAN or ERSPAN sessions, use the **no** form of this command.

monitor session {*session-number* [**shut** | **type** {**local** | **erspan-destination** | **erspan-source**}] | **all** **shut**}

no monitor session {*session-number* | **all**} [**shut**]

Syntax Description

<i>session-number</i>	SPAN session to create or configure. The range is from 1 to 18.
all	Specifies to apply configuration information to all SPAN sessions.
shut	(Optional) Specifies that the selected session will be shut down for monitoring.
type	(Optional) Specifies the type of session to configure.
local	Specifies the session type to be local.
erspan-destination	Creates an ERSPAN destination session.
erspan-source	Creates an ERSPAN source session.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U2(2)	Support for ERSPAN was added.

Usage Guidelines

To ensure that you are working with a completely new session, you can clear the desired session number or all SPAN sessions.

After you create an ERSPAN session, you can describe the session and add interfaces and VLANs as sources and destinations.

This command does not require a license.

Examples

This example shows how to create a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config)#
```


Send comments to nexus3k-docfeedback@cisco.com

This example shows how to enter the monitor configuration mode for configuring SPAN session number 9 for analyzing traffic between ports:

```
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)# destination interface ethernet 1/2
switch(config-monitor)# no shutdown
switch(config-monitor)#
```

This example shows how to configure any SPAN destination interfaces as Layer 2 SPAN monitor ports before activating the SPAN session:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# no shutdown
switch(config-if)#
```

This example shows how to configure a typical SPAN destination trunk interface:

```
switch# configure terminal
switch(config)# interface Ethernet1/2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport monitor
switch(config-if)# switchport trunk allowed vlan 10-12
switch(config-if)# no shutdown
switch(config-if)#
```

This example shows how to create an ERSPAN session:

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

Related Commands

Command	Description
description (SPAN, ERSPAN)	Adds a description to identify the SPAN session.
destination (ERSPAN)	Configures the destination IP port for an ERSPAN packet.
ip dscp (ERSPAN)	Sets the DSCP value for an ERSPAN packet.
ip ttl (ERSPAN)	Sets the time-to-live (TTL) value for an ERSPAN packet.
mtu (ERSPAN)	Sets the maximum transmission value (MTU) for ERSPAN packets.
show monitor session	Displays SPAN session configuration information.
source (SPAN, ERSPAN)	Adds a SPAN source port.

Send comments to nexus3k-docfeedback@cisco.com

mpls strip dest-mac

To configure the destination MAC address for stripped egress frames, use the **mpls strip dest-mac** command. To delete the configured destination MAC address, use the **no** form of this command.

mpls strip dest-mac *mac-address*

no mpls strip dest-mac *mac-address*

Syntax Description

<i>mac-address</i>	Specifies the destination MAC address for egress frames that are stripped of their headers. The MAC address can be specified in one of the following four forms: <ul style="list-style-type: none"> • E.E.E • EE-EE-EE-EE-EE-EE • EE:EE:EE:EE:EE:EE • EEEE.EEEE.EEEE
--------------------	---

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)U2(5)	This command was introduced.

Examples

This example shows how to configure the destination MAC address for egress frames:

```
switch# configure terminal
switch(config)# mpls strip dest-mac 1.1.1
```

Related Commands

Command	Description
mpls strip	Enables the MPLS stripping feature.
clear mpls strip label dynamic	Clears dynamic label entries.
mpls strip label	Adds or deletes static MPLS labels.
mpls strip label-age	Configures MPLS label aging.
show mpls strip labels	Displays MPLS label configuration.

Send comments to nexus3k-docfeedback@cisco.com

mpls strip

To enable the MPLS stripping feature globally, use the **mpls strip** command. To disable this feature, use the **no** form of this command.

mpls strip

no mpls strip

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

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

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

Command History	Release	Modification
	6.0(2)U2(5)	This command was introduced.

Examples	This example shows how to enable MPLS stripping:
-----------------	--

```
switch# configure terminal
switch(config)# mpls strip
switch(config)#
```

This example shows how to disable MPLS stripping:

```
switch# configure terminal
switch(config)# no mpls strip
switch(config)#
```

Related Commands	Command	Description
	mpls strip label	Adds or deletes static MPLS labels.
	clear mpls strip label dynamic	Clears dynamic label entries.
	mpls strip label-age	Configures MPLS label aging.
	mpls strip dest-mac	Configures the destination MAC address for stripped egress frames.
	show mpls strip labels	Displays MPLS label configuration.

Send comments to nexus3k-docfeedback@cisco.com

mpls strip label

To add a static MPLS label, use the **mpls strip label** command. To delete a static MPLS label, use the **no** form of this command.

mpls strip label *label*

no mpls strip label *label* | **all**

Syntax Description

<i>label</i>	Specifies the value of the static MPLS label. The value of the label can range from 1 to 1048575. An MPLS label table can store up to 1025 static labels. The total number of labels that the table can store, including dynamic labels, is 15000.
all	Specifies that all static MPLS labels are to be deleted.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)U2(5)	This command was introduced.

Usage Guidelines

Before adding static labels to the MPLS label table, ensure the following:

- Tap Aggregation is enabled.
- Tap Aggregation policy is configured.
- The Tap aggregation policy is attached to an interface.

You can store up to 1025 static labels in an MPLS label table. However, the table can store up to 15000 labels, including dynamic labels.

Examples

This example shows how to add a static MPLS label:

```
switch# configure terminal
switch(config)# mpls strip label 100
switch(config)#
```

This example shows how to delete a static MPLS label:

```
switch# configure terminal
switch(config)# no mpls strip label 100
switch(config)#
```

Send comments to nexus3k-docfeedback@cisco.com

This example shows how to delete all static MPLS labels:

```
switch# configure terminal
switch(config)# no mpls strip label all
```

Related Commands

Command	Description
mpls strip	Enables the MPLS stripping feature.
clear mpls strip label dynamic	Clears dynamic label entries.
mpls strip label-age	Configures MPLS label aging.
mpls strip dest-mac	Configures the destination MAC address for stripped egress frames.
show mpls strip labels	Displays MPLS label configuration.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

mpls strip label-age

To define the amount of time after which dynamic MPLS labels age out, use the **mpls strip label-age** command. To delete the defined age, use the **no** form of this command.

mpls strip label-age *age*

no mpls strip label-age *age*

Syntax Description	<i>age</i>	Specifies the amount of time after which dynamic MPLS labels age out. The value of the age can range from 1 to 10000000 seconds. The default age is 1800 seconds.
---------------------------	------------	--

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

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

Command History	Release	Modification
	6.0(2)U2(5)	This command was introduced.

Examples	<p>This example shows how to configure label age for dynamic MPLS labels:</p> <pre>switch# configure terminal switch(config)# mpls strip label-age 300 switch(config)#</pre>
-----------------	--

Related Commands	Command	Description
	mpls strip	Enables the MPLS stripping feature.
	clear mpls strip label dynamic	Clears dynamic label entries.
	mpls strip label	Adds or deletes static MPLS labels.
	mpls strip dest-mac	Configures the destination MAC address for stripped egress frames.
	show mpls strip labels	Displays MPLS label configuration.

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Usage Guidelines	You can specify multiple peer associations.
------------------	---

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

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

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

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

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

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

Send comments to nexus3k-docfeedback@cisco.com

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

Send comments to nexus3k-docfeedback@cisco.com

ntp abort

To discard the Network Time Protocol (NTP) configuration, 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
	5.0(3)U1(1)	This command was introduced.

Examples	This example shows how to abort the NTP configuration:
-----------------	--

<pre>switch# configure terminal switch(config)# ntp abort switch(config)#</pre>

Related Commands	Command	Description
	ntp distribute	Enables CFS distribution for NTP.
	show ntp	Displays NTP information.
	ntp commit	Commits the NTP configuration.

Send comments to nexus3k-docfeedback@cisco.com

ntp access-group

To configure an access group to control Network Time Protocol (NTP) access, use the **ntp access-group** command. To remove the NTP peer access group, use the **no** form of this command.

ntp access-group { **peer** | **serve** | **serve-only** | **query-only** } *access-list-name*

no ntp access-group { **peer** | **serve** | **serve-only** | **query-only** } *access-list-name*

Syntax Description

peer	Allows the device to receive time requests and NTP control queries to synchronize itself to the servers specified in the access list.
serve	Allows the device to receive time requests and NTP control queries from the servers specified in the access list but not to synchronize itself to the specified servers.
serve-only	Allows the device to receive only time requests from servers specified in the access list.
query-only	Allows the device to receive only NTP control queries from the servers specified in the access list.
<i>access-list-name</i>	Name of the NTP access group. The name can be any alphanumeric string up to 32 characters, including special characters.

Defaults

If you do not configure any access groups, NTP access is granted to all devices.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

The **ntp access-group match-all** command causes the access group options to be scanned in the following order, from least restrictive to most restrictive: peer, serve, serve-only, query-only. If the incoming packet does not match the peer access group, the packet goes to the serve access group to be processed. If the packet does not match the serve access group, it goes to the next access group and so on. This command also enables IPv6 access group processing.

This command does not require a license.

Examples

This example shows how to configure a peer access group for NTP:

```
switch# configure terminal
switch(config)# ntp access-group peer Admin_Group_123
switch(config)#
```

This example shows how to remove an NTP peer access group:

```
switch# configure terminal
```

Send comments to nexus3k-docfeedback@cisco.com

```
switch(config)# no ntp access-group peer Admin_Group_123
switch(config)#
```

Related Commands

Command	Description
show ntp access-groups	Displays the NTP access groups.

Send comments to nexus3k-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.

Defaults Disabled

Command Modes Global configuration mode

Command History	Release	Modification
	6.0(2)U(2)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
switch(config)#
```

This example shows how to disable NTP authentication:

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

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	ntp authentication-key	Configures an NTP authentication key.
	ntp trusted-key	Configures one or more keys that a time source must provide in its NTP packets in order for the device to synchronize to it.
	show ntp authentication-status	Displays the status of NTP authentication.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

ntp authentication-key

To configure a Network Time Protocol (NTP) authentication key, use the **ntp authentication-key** command. To remove the NTP authentication key, use the **no** form of this command.

ntp authentication-key *number*

no ntp authentication-key *number*

Syntax Description	<i>number</i> Authentication key number. The range is from 1 to 65535.	
Defaults	Disabled	
Command Modes	Global configuration mode	
Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.
Usage Guidelines	<p>The device does not synchronize to a time source unless the source has one of these authentication keys and the key number is specified by the ntp trusted-key command.</p> <p>This command does not require a license.</p>	
Examples	<p>This example shows how to configure an NTP authentication key:</p> <pre>switch# configure terminal switch(config)# ntp authentication-key 42 switch(config)#</pre> <p>This example shows how to remove the NTP authentication key:</p> <pre>switch# configure terminal switch(config)# no ntp authentication-key 42 switch(config)#</pre>	
Related Commands	Command	Description
	show ntp authentication-key	Configures one or more keys that a time source must provide in its NTP packets in order for the device to synchronize to it.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

ntp broadcast

To enable a Network Time Protocol (NTP) IPv4 broadcast server on the specified interface, use the **ntp broadcast** command. To disable the NTP IPv4 broadcast server, use the **no** form of this command.

ntp broadcast [*destination ip-address*] [*key key-id*] [*version number*]

no ntp broadcast [*destination ip-address*] [*key key-id*] [*version number*]

Syntax Description

destination <i>ip-address</i>	(Optional) Configures the broadcast destination IPv4 address.
key <i>key-id</i>	(Optional) Configures the broadcast authentication key number. The range is from 1 to 65535.
version <i>number</i>	(Optional) Configures the NTP version. The range is from 2 to 4.

Defaults

None

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

Use NTP broadcast or multicast associations when time accuracy and reliability requirements are modest, your network is localized, and the network has more than 20 clients. We recommend that you use NTP broadcast or multicast associations in networks that have limited bandwidth, system memory, or CPU resources.



Note

Time accuracy is marginally reduced in NTP broadcast associations because information flows only one way.

This command does not require a license.

Examples

This example shows how to enable an NTP IPv4 broadcast server on the interface:

```
switch# configure terminal
switch(config)# interface ethernet 6/1
switch(config-if)# ntp broadcast destination 192.0.2.10
```

Send comments to nexus3k-docfeedback@cisco.com

ntp broadcastdelay

To configure the estimated Network Time Protocol (NTP) broadcast round-trip delay, use the **ntp broadcastdelay** command. To disable the estimated broadcast round-trip delay, use the **no** form of this command.

ntp broadcastdelay [*delay*]

no ntp broadcastdelay [*delay*]

Syntax Description	<i>delay</i> (Optional) Broadcast round-trip delay in microseconds. The range is from 1 to 999999.
---------------------------	--

Defaults	None
-----------------	------

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

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines	Use NTP broadcast or multicast associations when time accuracy and reliability requirements are modest, your network is localized, and the network has more than 20 clients. We recommend that you use NTP broadcast or multicast associations in networks that have limited bandwidth, system memory, or CPU resources.
-------------------------	--



Note

Time accuracy is marginally reduced in NTP broadcast associations because information flows only one way.

This command does not require a license.

Examples	This example shows how to configure the estimated broadcast round-trip delay:
-----------------	---

```
switch# configure terminal
switch(config-if)# ntp broadcastdelay 100
```


Send comments to nexus3k-docfeedback@cisco.com

ntp commit

To apply the pending configuration pertaining to the Network Time Protocol (NTP) distribution session in progress, 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
	6.0(2)U2(1)	This command was introduced.

Examples	This example shows how to commit changes to the active NTP configuration:
-----------------	---

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

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

Send comments to nexus3k-docfeedback@cisco.com

ntp disable

To disable Network Time Protocol (NTP), use the **ntp disable** command. To reenable NTP, use the **no** form of this command.

ntp disable {ip | ipv6}

no ntp disable {ip | ipv6}

Syntax Description	ip	Disables IPv4 on the interface.
	ipv6	Disables IPv6 on the interface.

Defaults	Enabled
----------	---------

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

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines	This command does not require a license.
------------------	--

Examples	This example shows how to disable NTP: switch# ntp disable
----------	--

Send comments to nexus3k-docfeedback@cisco.com

ntp distribute

To enable configuration 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
	6.0(2)U2(1)	This command was introduced.

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

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

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

ntp logging

To enable Network Time Protocol (NTP) logging, use the **ntp logging** command. To disable NTP logging, use the **no** form of this command.

ntp logging

no ntp logging

Syntax Description This command has arguments or keywords.

Defaults Disabled

Command Modes Global configuration mode (config)

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to enable NTP logging:

```
switch# configure terminal
switch(config)# ntp logging
switch(config)#
```

This example shows how to disable NTP logging:

```
switch# configure terminal
switch(config)# no ntp logging
switch(config)#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	show ntp logging-status	Displays the NTP logging status.
	show ntp statistics	Displays the NTP statistics.

Send comments to nexus3k-docfeedback@cisco.com

ntp master

To configure the device to act as an authoritative Network Time Protocol (NTP) server, use the **ntp master** command. To remove the device as an authoritative NTP server, use the **no** form of this command.

ntp master [*stratum*]

no ntp master [*stratum*]

Syntax Description

stratum (Optional) Stratum number. The range is from 1 to 15.

Defaults

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This command enables the device to distribute time even when it is not synchronized to an existing time server.

This command does not require a license.

Examples

This example shows how to configure the device to act as an authoritative NTP server:

```
switch# configure terminal
switch(config)# feature ntp
switch(config)# ntp master 5
```

This example shows how to remove a device as an authoritative NTP server:

```
switch# configure terminal
switch(config)# no ntp master 5
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	show running-config ntp	Displays information about the NTP configuration that is currently running on the switch.

Send comments to nexus3k-docfeedback@cisco.com

ntp multicast

To enable an Network Time Protocol (NTP) IPv4 or IPv6 multicast server on the interface, use the **ntp multicast** command. To disable an NTP multicast server on the interface, use the **no** form of this command.

ntp multicast [*ipv4-address* | *ipv6 address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*]

no ntp multicast [*ipv4-address* | *ipv6 address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*]

Syntax Description

<i>ip4-address</i>	(Optional) Multicast IPv4 address.
<i>ipv6-address</i>	(Optional) Multicast IPv6 address.
key <i>key-id</i>	(Optional) Configures the broadcast authentication key number. The range is from 1 to 65535.
ttl <i>value</i>	(Optional) Configures the time-to-live (TTL) value of the multicast packets. The range is from 1 to 255
version <i>number</i>	(Optional) Configures the NTP version. The range is from 2 to 4.

Defaults

None

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

You can use the **ntp multicast** command to configure an NTP IPv4 or IPv6 multicast server on an interface. The device then sends multicast packets through that interface periodically.

Use NTP broadcast or multicast associations when time accuracy and reliability requirements are modest, your network is localized, and the network has more than 20 clients. We recommend that you use NTP broadcast or multicast associations in networks that have limited bandwidth, system memory, or CPU resources.

This command does not require a license.

Examples

This example shows how to configure an NTP IPv6 multicast server on an interface:

```
switch(config)# interface ethernet 6/1
switch(config-if)# ntp multicast FF02:1::FF0E:8C6C
```


Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	ntp multicast client	Configures an NTP multicast client on an interface.
	show running-config ntp	Displays information about the NTP configuration that is currently running on the switch.

Send comments to nexus3k-docfeedback@cisco.com

ntp multicast client

To configure a Network Time Protocol (NTP) multicast client on an interface, use the **ntp multicast client** command. To disable an NTP multicast client on the interface, use the **no** form of this command.

ntp multicast client [*ipv4-address* | *ipv6 address*]

no ntp multicast client [*ipv4-address* | *ipv6 address*]

Syntax Description	<i>ipv4-address</i>	(Optional) Multicast IPv4 address.
	<i>ipv6-address</i>	(Optional) Multicast IPv6 address.

Defaults	None
-----------------	------

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

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines

You can use the **ntp multicast client** command to configure an NTP multicast client on an interface. The device then listens to NTP multicast messages and discards any messages that come from an interface for which multicast is not configured.

Use NTP broadcast or multicast associations when time accuracy and reliability requirements are modest, your network is localized, and the network has more than 20 clients. We recommend that you use NTP broadcast or multicast associations in networks that have limited bandwidth, system memory, or CPU resources.

This command does not require a license.

Examples

This example shows how to configure an NTP IPv6 multicast server on an interface:

```
switch(config)# interface ethernet 6/1
switch(config-if)# ntp multicast client FF02:1::FF0E:8C6C
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	ntp multicast	Configures an NTP multicast server on an interface.
	show running-config ntp	Displays information about the NTP configuration that is currently running on the switch.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

ntp peer

To configure a device as a Network Time Protocol (NTP) peer, use the **ntp peer** command. To remove the device as an NTP peer, use the **no** form of this command.

ntp peer { *ip-address* | *ipv6-address* | *dns-name* }

no ntp peer { *ip-address* | *ipv6-address* | *dns-name* }

Syntax Description

<i>ip-address</i>	IPv4 address.
<i>ipv6-address</i>	IPv6 address.
<i>dns-name</i>	Domain Name Server (DNS) name.

Defaults

None

Command Modes

Global configuration mode (config)

Command History

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

Usage Guidelines

You can configure multiple peer associations.
This command does not require a license.

Examples

This example shows how to configure an NTP peer:

```
switch(config)# configure terminal
switch(config)# ntp peer 190.0.2.1
switch(config)#
```

This example shows how to remove an NTP peer:

```
switch# configure terminal
switch(config)# no ntp peer 190.0.2.1
switch(config)#
```

Related Commands

Command	Description
ntp server	Configures an NTP server.
show ntp peers	Displays all the NTP peers.
show ntp peer-status	Displays the status for all the server/peers.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

ntp server

To configure a Network Time Protocol (NTP) server, use the **ntp server** command. To remove the NTP server, use the **no** form of this command.

ntp server {*ip-address* | *ipv6-address* | *dns-name*}

no ntp server {*ip-address* | *ipv6-address* | *dns-name*}

Syntax Description	<i>ip-address</i>	IPv4 address.
	<i>ipv6-address</i>	IPv6 address.
	<i>dns-name</i>	Domain Name Server (DNS) name.

Defaults	None
----------	------

Command Modes	Global configuration mode (config)
---------------	------------------------------------

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines	This command does not require a license.
------------------	--

Examples This example shows how to configure an NTP server:

```
switch(config) configure terminal  
switch(config)# ntp server 190.0.2.10  
switch(config)#
```

This example shows how to remove an NTP server:

```
switch# configure terminal  
switch(config)# no ntp server 190.0.2.10  
switch(config)#
```

Related Commands	Command	Description
	ntp peer	Configures a device as an NTP peer.
	show ntp peer-status	Displays the status of all NTP servers and peers.
	show ntp peers	Displays all the NTP peers.

Send comments to nexus3k-docfeedback@cisco.com

ntp source

To configure the Network Time Protocol (NTP) source, use the **ntp source** command. To remove the NTP source, use the **no** form of this command.

ntp source *addr*

no ntp source *addr*

Syntax Description	<i>addr</i> IPv4 or IPv6 address of the source. The IPv4 address format is dotted decimal, x.x.x.x. The IPv6 address format is hex A:B::C:D.	
Defaults	None	
Command Modes	Global configuration mode	
Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	<p>This example shows how to configure the NTP source:</p> <pre>switch(config)# ntp source 192.0.2.3</pre> <p>This example shows how to remove the NTP source:</p> <pre>switch(config)# no ntp source 192.0.2.3</pre>	
Related Commands	Command	Description
	show ntp source	Displays information about the NTP source.

Send comments to nexus3k-docfeedback@cisco.com

ntp source-interface

To configure the Network Time Protocol (NTP) source interface, use the **ntp source-interface** command. To remove an NTP source interface, use the **no** form of this command.

ntp source-interface *type interface-number*

no ntp source-interface *type interface-number*

Syntax Description	<i>type</i>	Source interface.
	<i>interface-number</i>	Source interface number for the source type:
	<i>ether</i>	ethernet—Slot/chassis number. The range is from 1 to 255.
		loopback—Virtual interface number. The range is from 1 to 1023.
		mgmt—Management interface number.
		port-channel—Port Channel number. The range is from 1 to 4096.
		vlan—VLAN interface number. The range is from 1 to 4094.
Defaults	None	
Command Modes	Global configuration mode	
Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example shows how to configure an NTP source interface:	
	<pre>switch(config)# ntp source-interface loopback 1 switch(config)#</pre>	
	This example shows how to remove an NTP source configuration:	
	<pre>switch(config)# no ntp source-interface loopback 1 switch(config)#</pre>	
	Command	Description
	show ntp source-interface	Displays information about the NTP source interface.

Send comments to nexus3k-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
	6.0(2)U2(1)	This command was introduced.

Examples	This example shows how to retry synchronization with the configured NTP servers:
-----------------	--

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

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

Send comments to nexus3k-docfeedback@cisco.com

ntp trusted-key

To configure one or more keys that a time source must provide in its Network Time Protocol (NTP) packets in order for the device to synchronize to it, use the **ntp trusted-key** command. To remove the NTP trusted key, use the **no** form of this command.

ntp trusted-key *number*

no ntp trusted-key *number*

Syntax Description

<i>number</i>	Trusted key number. The range is from 1 to 65535.
---------------	---

Defaults

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

This command provides protection against accidentally synchronizing the device to a time source that is not trusted.

This command does not require a license.

Examples

This example shows how to configure an NTP trusted key:

```
switch# configure terminal
switch(config)# ntp trusted-key 42
switch(config)#
```

This example shows how to remove the NTP trusted key:

```
switch# configure terminal
switch(config)# no ntp trusted-key 42
switch(config)#
```

Related Commands

Command	Description
show ntp trusted-keys	Displays the status of NTP authentication.

Send comments to nexus3k-docfeedback@cisco.com

periodic-inventory (Call Home)

To configure the switch to periodically send a message with an inventory of all software services currently enabled and running on the device with hardware inventory information, use the **periodic-inventory** command. To disable the periodic messages, use the **no** form of this command.

periodic-inventory notification [**interval** *time-period* | **timeofday** *time-of-day*]

no periodic-inventory notification [**interval** *time-period* | **timeofday** *time-of-day*]

Syntax Description

notification	Enables sending periodic software inventory messages.
interval <i>time-period</i>	(Optional) Specifies the time period for periodic inventory notification. The time period range is from 1 to 30 days, and the default is 7 days.
timeofday <i>time-of-day</i>	(Optional) Specifies the time of day for periodic inventory notification. The time of day is in HH:MM format.

Command Default

Interval: 7 days

Command Modes

Callhome configuration mode

Command History

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

Usage Guidelines

The switch generates two Call Home notifications: periodic configuration messages and periodic inventory messages.

Examples

This example shows how to configure a periodic inventory notification to generate every 5 days:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# periodic-inventory notification interval 5
switch(config-callhome)#
```

This example shows how to disable a periodic inventory notification for Call Home:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# no periodic-inventory notification interval 5
switch(config-callhome)#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	copy running-config startup-config	Saves this configuration change.
	show callhome	Displays Call Home configuration information.
	show running-config callhome	Displays the running configuration information for Call Home.

Send comments to nexus3k-docfeedback@cisco.com

phone-contact (Call Home)

To configure the phone number for the primary person responsible for the device, use the **phone-contact** command. To remove a phone contact, use the **no** form of this command.

phone-contact *phone-no*

no phone-contact

Syntax Description	<i>phone-no</i>	Phone number in international phone number format, such as +1-800-123-4567. The phone number can be a maximum of 17 alphanumeric characters and cannot contain spaces.
	Note	You must use the + prefix before the number.

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

Command Modes	Callhome configuration mode
----------------------	-----------------------------

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

Examples	<p>This example shows how to configure a phone number for the primary person responsible for the device:</p> <pre>switch# configure terminal switch(config)# callhome switch(config-callhome)# phone-contact +1-800-123-4567 switch(config-callhome)#</pre>
-----------------	--

Related Commands	Command	Description
	copy running-config startup-config	Saves this configuration change.
	show callhome	Displays a summary of the Call Home configuration.
	streetaddress	Configures the street address for the primary person responsible for the switch.

Send comments to nexus3k-docfeedback@cisco.com

ptp

To enable the Precision Time Protocol (PTP) on an interface, use the **ptp** command. To disable PTP on an interface, use the **no** form of this command.

ptp

no ptp

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Interface configuration mode

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to enable PTP on an interface:

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

This example shows how to disable PTP on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no ptp
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 source	Configures the source IP address for all PTP packets.
	ptp sync interval	Configures the interval between PTP synchronization messages on an interface.
	ptp vlan	Configures the PTP VLAN value on an interface.

Send comments to nexus3k-docfeedback@cisco.com

ptp announce

To configure the interval between Precision Time Protocol (PTP) announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface, use the **ptp announce** command. To remove the interval configuration for PTP messages, use the **no** form of this command.

ptp announce {*interval seconds* | *timeout count*}

no ptp announce {*interval seconds* | *timeout count*}

Syntax Description

interval	Specifies the interval between Precision Time Protocol (PTP) announce messages on an interface.
<i>seconds</i>	Log seconds. The range is from 0 to 4.
timeout	Specifies the number of PTP intervals before a timeout occurs on an interface.
<i>count</i>	Timeout count. The range is from 2 to 10. Beginning in Release 7.0(3)I2(1), the value is 2 to 4.

Command Default

interval 1
timeout 3

Command Modes

Interface configuration mode

Command History

Release	Modification
7.0(3)I2(1)	The count changed to 2 to 4.
5.0(3)U2(2)	This command was introduced.

Usage Guidelines

Make sure that you have globally enabled PTP on the switch and configured the source IP address for PTP communication.

This command does not require a license.

Examples

This example shows how to configure the interval between PTP announce messages on an interface:

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

This example shows how to remove the interval configuration for PTP messages from an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no ptp announce interval 1
switch(config-if)#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	feature ptp	Enables or disables PTP on the device.
	ptp	Enables or disables PTP 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 source	Configures the source IP address for all PTP packets.
	ptp sync interval	Configures the interval between PTP synchronization messages on an interface.
	ptp vlan	Configures the PTP VLAN value on an interface.

Send comments to nexus3k-docfeedback@cisco.com

ptp delay-request minimum interval

To configure the minimum interval allowed between Precision Time Protocol (PTP) delay-request messages when the port is in the master state, use the **ptp delay-request minimum interval** command. To remove the minimum interval configuration for PTP delay-request messages, use the **no** form of this command.

ptp delay-request minimum interval *seconds*

no ptp delay-request minimum interval *seconds*

Syntax Description	<i>seconds</i>	Log seconds. The range is from -1 to 6.
---------------------------	----------------	---

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

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

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines	Make sure that you have globally enabled PTP on the switch and configured the source IP address for PTP communication.
-------------------------	--

This command does not require a license.

Examples	This example shows how to configure the minimum interval allowed between PTP delay-request messages:
-----------------	--

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

This example shows how to remove the minimum interval configuration for PTP delay-request messages:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no ptp delay-request minimum interval 3
switch(config-if)#
```

Related Commands	Command	Description
	feature ptp	Enables or disables PTP on the device.
	ptp	Enables or disables PTP on an interface.

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
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 source	Configures the source IP address for all PTP packets.
ptp sync interval	Configures the interval between PTP synchronization messages on an interface.
ptp vlan	Configures the PTP VLAN value on an interface.

Send comments to nexus3k-docfeedback@cisco.com

ptp domain

To configure a domain number for the Precision Time Protocol (PTP) clock, use the **ptp domain** command. To remove the domain configuration for the PTP clock, use the **no** form of this command.

ptp domain *domain_number*

no ptp domain *domain_number*

Syntax Description

<i>domain_number</i>	Domain number. The range is from 0 to 128.
----------------------	--

Command Default

0

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(3)U2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a domain number for the PTP clock:

```
switch# configure terminal
switch(config)# ptp domain 6
switch(config)#
```

This example shows how to remove the PTP domain configuration:

```
switch# configure terminal
switch(config)# no ptp domain 6
switch(config)#
```

Related Commands

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

ptp priority1

To configure the priority1 value when advertising the Precision Time Protocol (PTP) clock, use the **ptp priority1** command. To remove the priority1 value, use the **no** form of this command.

ptp priority1 *priority-number*

no ptp priority1 *priority-number*

Syntax Description	<i>priority-number</i>	Priority number. The range is from 0 to 255.
---------------------------	------------------------	--

Command Default	255
------------------------	-----

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

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to configure the priority1 value when advertising the PTP clock:
-----------------	---

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

This example shows how to remove the priority1 value when advertising the PTP clock:

```
switch# configure terminal
switch(config)# no ptp priority1 10
switch(config)#
```

Related Commands	Command	Description
	feature ptp	Enables or disables PTP on the switch.
	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 nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

ptp priority2

To configure the priority2 value when advertising the Precision Time Protocol (PTP) clock, use the **ptp priority2** command. To remove the priority2 value when advertising the PTP, use the **no** form of this command.

ptp priority2 *priority-number*

no ptp priority2 *priority-number*

Syntax Description	<i>priority-number</i> Priority number. The range is from 0 to 255.	
Command Default	255	
Command Modes	Global configuration mode	
Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example shows how to configure the priority2 value when advertising the PTP clock:	
	<pre>switch# configure terminal switch(config)# ptp priority2 1 switch(config)#</pre>	
	This example shows how to remove the priority2 value configuration for use when advertising the PTP clock:	
	<pre>switch# configure terminal switch(config)# no ptp priority2 1 switch(config)#</pre>	
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 nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

ptp source

To configure the global source for all the Precision Time Protocol (PTP) packets, use the **ptp source** command. To remove the global source for PTP packets, use the **no** form of this command.

ptp source *ip_address* [**vrf** {*vrf-name* | **management**}]

no ptp source *ip_address* [**vrf** {*vrf-name* | **management**}]

Syntax Description	<i>ip_address</i>	IPv4 address of the source.
	vrf	Specifies the virtual routing and forwarding (VRF) instance.
	<i>vrf-name</i>	Name of the VRF. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
	management	Specifies the management VRF.

Command Default None

Command Modes Global configuration mode

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines This command does not require a license.

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

```
switch# configure terminal
switch(config)# ptp source 192.0.1.1
switch(config)#
```

This example shows how to remove the global source configuration for all the PTP packets:

```
switch# configure terminal
switch(config)# no ptp source 192.0.1.1
switch(config)#
```

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 priority1 value to use when advertising this clock.
	ptp priority2	Configures the priority2 value to use when advertising this clock.

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
show ptp brief	Displays the PTP status.
show ptp clock	Displays the properties of the local clock.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

ptp sync interval

To configure the interval between Precision Time Protocol (PTP) synchronization messages on an interface, use the **ptp sync interval** command. To remove the interval configuration for PTP messages synchronization, use the **no** form of this command.

ptp sync interval *seconds*

no ptp sync interval *seconds*

Syntax Description	<i>seconds</i>	Log seconds. The range is from -6 to 1. Beginning in Release 7.0(3)I2(1), the value is -3 to 1.
---------------------------	----------------	---

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

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

Command History	Release	Modification
	7.0(3)I2(1)	The <i>seconds</i> value is now -3 to 1.
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines	Make sure that you have globally enabled PTP on the switch and configured the source IP address for PTP communication.
	A Cisco Nexus 3000 Series switch must be synchronized on the Slave port with a sync log interval value of less than or equal to -3. Any Master ports on the switch that are connected to downlink Cisco Nexus 3000 Series switches must be configured for a sync log interval value that is less than or equal to -3.
	This command does not require a license.

Examples	This example shows how to configure the interval between PTP synchronization messages on an interface:
-----------------	--

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

This example shows how to remove the interval configuration for PTP messages synchronization:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no ptp sync interval 1
switch(config-if)#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	feature ptp	Enables or disables PTP on the switch.
	ptp	Enables or disables PTP on an interface.
	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 PTP VLAN value on an interface.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

ptp vlan

To configure a VLAN to generate the Precision Time Protocol (PTP) messages for Layer 2 interfaces, use the **ptp vlan** command. To remove the PTP VLAN configuration from an interface, use the **no** form of this command.

ptp vlan *vlan-number*

no ptp vlan *vlan-number*

Syntax Description

<i>vlan-number</i>	VLAN number. The range is from 1 to 4094.
--------------------	---

Command Default

1

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(3)U2(2)	This command was introduced.

Usage Guidelines

Make sure that you have globally enabled PTP on the switch and configured the source IP address for PTP communication.

Use this command only on Layer 2 Ethernet interfaces (1 Gigabit, 10-Gigabit, 40-Gigabit) or port-channel members.

By default, VLAN 1 is used to generate the PTP messages on an interface. You must explicitly configure the following VLANs to generate PTP messages on interfaces:

- nondefault access VLANs on an access port
- nondefault native VLANs on a trunk port

This command does not require a license.

Examples

This example shows how to configure the PTP VLAN value on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# ptp vlan 9
switch(config-if)#
```

This example shows how to remove the PTP VLAN value from an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no vlan 9
switch(config-if)#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	feature ptp	Enables or disables PTP on the switch.
	ptp	Enables or disables PTP on an interface.
	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.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

rmon alarm

To configure Remote Monitoring (RMON) alarms on any integer-based Simple Network Management Protocol (SNMP) management information base (MIB) object, use the **rmon alarm** command. To remove an RMON alarm, use the **no** form of this command.

rmon alarm *alarm-no* *MIB-obj* *sample-interval* { **absolute** | **delta** } **rising-threshold** *rising-threshold-value* { *event-index* **falling-threshold** *fall-threshold-value* [*event-index*] [*owner name*] | **falling-threshold** *fall-threshold-value* [*event-index*] [*owner name*] }

no **rmon alarm** *alarm-no* *MIB-obj* *sample-interval* { **absolute** | **delta** } **rising-threshold** *rising-threshold-value* { *event-index* **falling-threshold** *fall-threshold-value* [*event-index*] [*owner name*] | **falling-threshold** *fall-threshold-value* [*event-index*] [*owner name*] }

Syntax Description		
<i>alarm-no</i>		Alarm number. The range is from 1 to 65535.
<i>MIB-obj</i>		MIB object to monitor. The MIB object must be an existing SNMP MIB object in standard dot notation; for example, 1.3.6.1.2.1.2.2.1.17.83886080.
<i>sample-interval</i>		Sample interval at which the switch collects a sample value of the MIB object. The range is from 1 to 700000 seconds.
absolute		Specifies the sample type as absolute.
delta		Specifies the sample type as delta.
rising-threshold		Configures the rising threshold value at which the switch triggers a rising alarm or resets a falling alarm.
<i>rising-threshold-value</i>		Rising threshold value. The range is from -2147483648 to 2147483647.
<i>event-index</i>		Event or action that the switch takes when an alarm, rising or falling, triggers. The <i>event index</i> range is from 0 to 65535.
falling-threshold		Configures the falling threshold value at which the switch triggers a falling alarm or resets a rising alarm.
<i>fall-threshold-value</i>		Falling threshold value. The range is from -2147483648 to 2147483647. Note The falling threshold value must be less than the rising threshold.
<i>owner name</i>		(Optional) Specifies an owner for the alarm. The name can be any alphanumeric string.

Command Default None

Command Modes Global configuration mode

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

Send comments to nexus3k-docfeedback@cisco.com

Usage Guidelines

Before you use this command, you must have configured an SNMP user and enabled SNMP notifications using the **snmp-server user** and **snmp-server enable traps** command, respectively.

You can only configure an RMON alarm on an integer-based SNMP MIB object. The MIB object must be in standard dot notation. For example, 1.3.6.1.2.1.2.2.1.17 represents ifOutOctets.17.

Absolute samples take the current snapshot of the MIB object value. Delta samples take two consecutive samples and calculate the difference between them. For example, you can set a delta type rising alarm on an error counter MIB object. If the error counter delta exceeds this value, you can trigger an event that sends an SNMP notification and logs the rising alarm event. This rising alarm will not occur again until the delta sample for the error counter drops below the falling threshold.

You can associate a particular event to each RMON alarm. RMON supports the following event types:

- **SNMP notification**—Sends an SNMP risingAlarm or fallingAlarm notification when the associated alarm triggers.
- **Log**—Adds an entry in the RMON log table when the associated alarm triggers.
- **Both**—Sends an SNMP notification and adds an entry in the RMON log table when the associated alarm triggers.

You can specify a different event for a falling alarm and a rising alarm.

Examples

This example shows how to configure an RMON alarm:

```
switch(config)# rmon alarm 1 1.3.6.1.2.1.2.2.1.17.83886080 5 delta rising-threshold 5 1
falling-threshold 0 owner test
switch(config)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
snmp-server enable traps	Enables SNMP notifications on the switch.
snmp-server user	Configures an SNMP user.
show rmon	Displays information about RMON alarms and events.

Send comments to nexus3k-docfeedback@cisco.com

rmon event

To configure Remote Monitoring (RMON) events to associate with RMON alarms, use the **rmon event** command. To remove an RMON event, use the **no** form of this command.

rmon event *event-index* [**description** *string*] [**log**] [**trap**] [**owner** *name*]

no rmon event *event-index* [**description** *string*] [**log**] [**trap**] [**owner** *name*]

Syntax Description	<i>event-index</i>	Event or action that the switch takes when an alarm, rising or falling, triggers. The <i>event index</i> range is from 0 to 65535.
	description <i>string</i>	(Optional) Specifies a description for the event. The description can be any alphanumeric string.
	log	(Optional) Specifies that an RMON log be generated when the event occurs.
	trap	(Optional) Specifies that an SNMP trap be generated when the event occurs.
	owner <i>name</i>	(Optional) Specifies an owner for the alarm. The name can be any alphanumeric string.

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

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

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

Usage Guidelines	<p>Before you use this command, you must have configured an SNMP user and enabled SNMP notifications using the snmp-server user and snmp-server enable traps command, respectively.</p> <p>You can reuse the same event with multiple RMON alarms.</p>
-------------------------	--

Examples	This example shows how to configure an RMON event:
-----------------	--

```
switch# configure terminal
switch(config)# rmon event 1 owner test
switch(config)#
```

Related Commands	Command	Description
	copy running-config startup-config	Saves the running configuration to the startup configuration file.
	snmp-server enable traps	Enables SNMP notifications on the switch.

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
snmp-server user	Configures an SNMP user.
show rmon	Displays information about RMON alarms and events.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

rmon hcalarm

To configure a high-capacity Remote Monitoring (RMON) alarm, use the **rmon hcalarm** command. To remove a high-capacity RMON alarm, use the **no** form of this command.

rmon hcalarm *alarm-no MIB-obj sample-interval* {**absolute** | **delta**} **startupalarm**
startup-alarm-type rising-threshold rising-threshold-value event-index falling-threshold
fall-threshold-value [event-index] [owner name]

no rmon hcalarm *alarm-no MIB-obj sample-interval* {**absolute** | **delta**} **startupalarm**
startup-alarm-type rising-threshold rising-threshold-value event-index falling-threshold
fall-threshold-value [event-index] [owner name]

Syntax Description	
<i>alarm-no</i>	Alarm number. The range is from 1 to 65535.
<i>MIB-obj</i>	MIB object to monitor. The MIB object must be an existing SNMP MIB object in standard dot notation; for example, 1.3.6.1.2.1.2.2.1.17.83886080.
<i>sample-interval</i>	Sample interval at which the switch collects a sample value of the MIB object. The range is from 1 to 700000 seconds.
absolute	Specifies the sample type as absolute.
delta	Specifies the sample type as delta.
startupalarm	Configures the startup alarm type.
<i>startup-alarm-type</i>	Startup alarm type. The range is from 1 to 3, where 1 is rising, 2 is falling, and 3 is rising or falling.
rising-threshold	Configures the rising threshold value at which the switch triggers a rising alarm or resets a falling alarm.
<i>rising-threshold-value</i>	Rising threshold value. The range is from 0 to 18446744073709551615.
<i>event-index</i>	Event or action that the switch takes when an alarm, rising or falling, triggers. The <i>event index</i> range is from 0 to 65535.
falling-threshold	Configures the falling threshold value at which the switch triggers a falling alarm or resets a rising alarm.
<i>fall-threshold-value</i>	Falling threshold value. The range is from 0 to 18446744073709551615. Note The falling threshold value must be less than the rising threshold.
owner name	(Optional) Specifies an owner for the alarm. The name can be any alphanumeric string.

Command Default None

Command Modes Global configuration mode

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

Send comments to nexus3k-docfeedback@cisco.com

Usage Guidelines

Before you use this command, you must have configured an SNMP user and enabled SNMP notifications using the **snmp-server user** and **snmp-server enable traps** command, respectively.

You can configure a high-capacity RMON alarm on any integer-based SNMP MIB object. The MIB object must be in standard dot notation. For example, 1.3.6.1.2.1.2.2.1.17 represents ifOutOctets.17.

Absolute samples take the current snapshot of the MIB object value. Delta samples take two consecutive samples and calculate the difference between them. For example, you can set a delta type rising alarm on an error counter MIB object. If the error counter delta exceeds this value, you can trigger an event that sends an SNMP notification and logs the rising alarm event. This rising alarm does not occur again until the delta sample for the error counter drops below the falling threshold.

You can associate a particular event to each high-capacity RMON alarm. RMON supports the following event types:

- **SNMP notification**—Sends an SNMP risingAlarm or fallingAlarm notification when the associated high-capacity alarm triggers.
- **Log**—Adds an entry in the RMON log table when the associated high-capacity alarm triggers.
- **Both**—Sends an SNMP notification and adds an entry in the RMON log table when the associated high-capacity alarm triggers.

You can specify a different event for a falling high-capacity alarm and a rising high-capacity alarm.

Examples

This example shows how to configure an RMON high-capacity alarm:

```
switch# configure terminal
switch(config)# rmon hcalarm 3 1.3.6.1.2.1.2.2.1.17.83886080 5 delta startupalarm 3
               rising-threshold 5 1 falling-threshold 3 3 owner test
switch(config)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
snmp-server enable traps	Enables SNMP notifications on the switch.
snmp-server user	Configures an SNMP user.
show rmon	Displays information about RMON alarms and events.

Send comments to nexus3k-docfeedback@cisco.com

scheduler

To create or schedule a scheduler job, use the **scheduler** command. To remove a job or scheduled job, use the **no** form of this command.

```
scheduler {aaa-authentication [username username] password [0 | 7] password |  
  job name job-name | logfile size filesize | schedule name schedule-name | transport email  
  [from email address] [reply to email address] [smtp-server]}
```

```
no scheduler {aaa-authentication [username username] password [0 | 7] password |  
  job name job-name | logfile size filesize | schedule name schedule-name | transport email  
  [from email address] [reply to email address] [smtp-server]}
```

Syntax Description		
aaa-authentication		Begins an AAA authentication exchange with a remote user.
username <i>username</i>		Indicates the remote user is entering a username and specifies the username. A username can be any case-sensitive, alphanumeric string up to 32 characters.
password		Indicates the remote user is entering a password for authentication.
0		Indicates the password is in clear text.
7		Indicates the password is encrypted.
<i>password</i>		Remote user's password. A password can be any case-sensitive, alphanumeric string up to 64 characters.
job name <i>job-name</i>		Places you into job configuration mode for the specified job name. The job name can be any alphanumeric string up to 31 characters.
logfile		Specifies a logfile configuration.
size <i>filesize</i>		Specifies the size of the logfile. The range is from 16 to 1024 KB.
schedule		Defines a schedule for a job.
name <i>schedule-name</i>		Specifies the name of the schedule. The schedule name can be any alphanumeric string up to 31 characters.
transport		Specifies transport-related configuration.
email		Specifies the e-mail address.
from <i>email address</i>		Configures the from e-mail address. An e-mail address can be up to 255 characters in this format: abc@xyz.com.
reply-to <i>email address</i>		Configures the reply to e-mail address. An e-mail address can be up to 255 character in this format: abc@xyz.com.
smtp-server		Specifies the Simple Mail Transport Protocol server, which can be a DNS name or an IPv4 or IPv6 address.

Defaults None

Command Modes Job configuration

Send comments to nexus3k-docfeedback@cisco.com

Command History

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

Usage Guidelines

To use the **scheduler** command, you must enable the scheduler. To enable the scheduler, use the **feature scheduler** command.

Remote users must authenticate with the device by using the **scheduler aaa-authentication** command before using the **scheduler** command to configure a maintenance job.



Note

The commands within a scheduler job must be entered in a single line separated by a semicolon (;).

Usage Guidelines

This command does not require a license.

Examples

This example shows how to create a scheduler job that saves the running configuration to a file in bootflash and then copies the file from bootflash to a TFTP server. The filename is created using the current timestamp and switch name.

```
switch(config)# scheduler job name backup-cfg
switch(config-job)# cli var name timestamp $(TIMESTAMP);copy running-config
bootflash:/${SWITCHNAME}-cfg.$(timestamp);copy bootflash:/${SWITCHNAME}-cfg.$(timestamp)
tftp://1.2.3.4/ vrf management
switch(config-job)# end
switch(config)#
```

This example shows how to remove a scheduler job:

```
switch(config)# no scheduler job name backup-cfg
```

This example shows how to schedule a scheduler job to run daily at 12:00 a.m.:

```
switch(config)# scheduler schedule name daily
switch(config-schedule)# job name backup-cfg
switch(config-schedule)# time daily 1:00
switch(config-schedule)# end
switch(config)#
```

This example shows how to remove a scheduler job schedule:

```
switch(config)# no scheduler schedule name daily
```

Related Commands

Command	Description
feature scheduler	Enables the scheduler.
show scheduler	Displays scheduler information.

Send comments to nexus3k-docfeedback@cisco.com

sflow agent-ip

To configure an IP address to the sFlow Agent, use the **sflow agent-ip** command. To remove the IP address, use the **no** form of this command.

sflow agent-ip *ip-address*

no sflow agent-ip *ip-address*

Syntax Description	<i>ip-address</i>	IPv4 address.
--------------------	-------------------	---------------

Defaults	None
----------	------

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

Command History	Release	Modification
	5.0(3)U4(1)	This command was introduced.

Usage Guidelines	You must specify a valid IP address to enable sFlow functionality. This command does not require a license.
------------------	--

Examples	This example shows how to configure the IPv4 address of the sFlow Agent. <pre>switch(config)# sflow agent-ip 192.0.2.3 switch(config)# copy running-config startup-config</pre>
----------	--

Related Commands	Command	Description
	feature sflow	Enables sFlow.
	show sflow	Displays sFlow information.

Send comments to nexus3k-docfeedback@cisco.com

sflow collector-ip

To configure the sFlow analyzer address, use the **sflow collector-ip** command. To remove the sFlow analyzer address, use the **no** form of this command.

sflow collector-ip *ip-address vrf-instance*

no sflow collector-ip *ip-address vrf-instance*

Syntax Description	<i>ip-address</i>	IPv4 address.
	<i>vrf-instance</i>	Specifies the virtual router context (VRF) instance. The VRF can be one of the following: <ul style="list-style-type: none"> <i>vrf-name</i>—VRF name. The name can be any case-sensitive, alphanumeric string up to 32 characters. vrf-default—Specifies the default VRF. vrf-management—Specifies the management VRF.
Defaults	None	
Command Modes	Global configuration	
Command History	Release	Modification
	5.0(3)U4(1)	This command was introduced.
Usage Guidelines	<p>You must use the vrf-management option if the sFlow data collector is on the network connected to the management port</p> <p>You must use the vrf-default option if the sFlow data collector is on the network connected to the front panel ports.</p> <p>This command does not require a license.</p>	
Examples	<p>This example shows how to configure the IPv4 address of the sFlow data collector that is connected to the management port.</p> <pre>switch# configure terminal switch(config)# sflow collector-ip 192.0.2.5 vrf-management switch(config)# copy running-config startup-config</pre>	
Related Commands	Command	Description
	feature sflow	Enables sFlow.
	show sflow	Displays sFlow information.

Send comments to nexus3k-docfeedback@cisco.com

sflow collector-port

To configure a destination port for the sFlow datagram, use the **sflow collector-port** command. To remove the destination port, use the **no** form of this command.

sflow collector-port *collector-port*

no sflow collector-port *collector-port*

Syntax Description	<i>collector-port</i> UDP port of the sFlow analyzer. The range for the <i>collector-port</i> is from 0 to 65535. The default value is 6343.	
Defaults	None	
Command Modes	Global configuration	
Command History	Release	Modification
	5.0(3)U4(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example shows how to configure the destination port for the sFlow datagrams. switch# configure terminal switch(config)# sflow collector-port 7000 switch(config)# copy running-config startup-config [#####] 100% switch(config)#	
Related Commands	Command	Description
	feature sflow	Enables sFlow.
	show sflow	Displays sFlow information.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

sflow counter-poll-interval

To configure an interval between sample counters associated with the datagram, use the **sflow collector-poll-interval** command. To remove the interval, use the **no** form of this command.

sflow counter-poll-interval *poll-interval*

no sflow counter-poll-interval *poll-interval*

Syntax Description	<i>poll-interval</i> Poll interval for an interface. The range for the <i>poll-interval</i> is from 0 to 2147483647 seconds. The default value is 20.	
Defaults	None	
Command Modes	Global configuration	
Command History	Release	Modification
	5.0(3)U4(1)	This command was introduced.
Usage Guidelines	A sampling interval of 0 disables counter sampling. This command does not require a license.	
Examples	This example shows how to configure the sFlow poll interval for an interface. <pre> switch# configure terminal switch(config)# sflow counter-poll-interval 100 switch(config)# copy running-config startup-config </pre>	
Related Commands	Command	Description
	feature sflow	Enables sFlow.
	show sflow	Displays sFlow information.

Send comments to nexus3k-docfeedback@cisco.com

sflow data-source

To configure a port or range of ports for the sFlow sampling data source, use the **sflow data-source** command. To remove the port, use the **no** form of this command.

sflow data-source interface [ethernet slot/port[-port] | port-channel channel-number]

no sflow data-source interface [ethernet slot/port[-port] | port-channel channel-number]

Syntax Description	<i>channel-number</i>	Specifies the Etherchannel number.
	ethernet slot/port[-port]	The slot or port or range of ports for an Ethernet data source.
	interface	Configures the Ethernet data source for the interfaces.
	port-channel	Specifies the Etherchannel interface.

Defaults None

Command Modes Global configuration

Command History	Release	Modification
	5.0(3)U4(1)	This command was introduced.

Usage Guidelines If you want to use a port channel as the data source, ensure that you have already configured the port channel and you know the port channel number.

This command does not require a license.

Examples This example shows how to configure Ethernet ports 5 through 12 for the sFlow sampler.

```
switch# configure terminal
switch(config)# sflow data-source interface ethernet 1/5-12
switch(config)# copy running-config startup-config
[#####] 100%
switch(config)#
```

This example shows how to configure port channel 100 for the sFlow sampler.

```
switch# configure terminal
switch(config)# sflow data-source interface port-channel 100
switch(config)# copy running-config startup-config
[#####] 100%
switch(config)#
```

Related Commands

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
feature sflow	Enables sFlow.
show sflow	Displays sFlow information.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

sflow max-datagram-size

To configure the maximum number of data bytes that can be sent in a single sample datagram, use the **sflow max-datagram-size** command. To remove the maximum of data bytes, use the **no** form of this command.

sflow max-datagram-size *datagram-size*

no sflow max-datagram-size *datagram-size*

Syntax Description	<i>datagram-size</i>	Maximum datagram size. The range for the <i>datagram-size</i> is from 200 to 9000 bytes. The default value is 1400.
---------------------------	----------------------	---

Defaults	None
-----------------	------

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

Command History	Release	Modification
	5.0(3)U4(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to configure sFlow maximum datagram size.
-----------------	--

```
switch# configure terminal
switch(config)# sflow maximum-datagram-size 2000
switch(config)# copy running-config startup-config
[#####] 100%
switch(config)#
```

Related Commands	Command	Description
	feature sflow	Enables sFlow.
	show sflow	Displays sFlow information.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

sflow max-sampled-size

To configure the maximum number of bytes copied from the sampled packet, use the **sflow max-sampled-size** command. To remove the maximum bytes, use the **no** form of this command.

sflow max-sampled-size *sampling-size*

no sflow max-sampled-size *sampling-size*

Syntax Description	<i>sampling-size</i> sFlow maximum sampling size packets. The range for the <i>sampling-size</i> is from 64 to 256 bytes. The default value is 128.							
Defaults	None							
Command Modes	Global configuration							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.0(3)U4(1)</td><td>This command was introduced.</td></tr></table>		Release	Modification	5.0(3)U4(1)	This command was introduced.		
Release	Modification							
5.0(3)U4(1)	This command was introduced.							
Usage Guidelines	This command does not require a license.							
Examples	<p>This example shows how to configure the maximum sampling size for the sFlow Agent.</p> <pre>switch# configure terminal switch(config)# sflow maximum-sampled-size 200 switch(config)# copy running-config startup-config</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>feature sflow</td><td>Enables sFlow.</td></tr><tr><td>show sflow</td><td>Displays sFlow information.</td></tr></table>		Command	Description	feature sflow	Enables sFlow.	show sflow	Displays sFlow information.
Command	Description							
feature sflow	Enables sFlow.							
show sflow	Displays sFlow information.							

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

sflow sampling-rate

To configure the sFlow sample rate for packets, use the **sflow sampling-rate** command. To remove the sample rate, use the **no** form of this command.

sflow sampling-rate *sampling-rate*

no sflow max-sampling-rate *sampling-rate*

Syntax Description	<i>sampling-rate</i> sFlow sampling rate for packets. The <i>sampling-rate</i> can be an integer between 4096 and 1000000000. The default value is 4096.	
Defaults	None	
Command Modes	Global configuration	
Command History	Release	Modification
	5.0(3)U4(1)	This command was introduced.
Usage Guidelines	A <i>sampling-rate</i> of 0 disables sampling. This command does not require a license.	
Examples	This example shows how to set the sampling rate to 50,000. switch# configure terminal switch(config)# sflow sampling-rate 50000 switch(config)# copy running-config startup-config	
Related Commands	Command	Description
	feature sflow	Enables sFlow.
	show sflow	Displays sFlow information.

Send comments to nexus3k-docfeedback@cisco.com

show callhome

To display the Call Home configuration information, use the **show callhome** command.

show callhome [**pending** | **pending-diff** | **session** | **status**]

Syntax Description		
pending	(Optional)	Displays the Call Home configuration changes in the pending Cisco Fabric Services (CFS) database.
pending-diff	(Optional)	Displays the differences between the pending and running Call Home configuration.
session	(Optional)	Displays the status of the last Call Home CFS command.
status	(Optional)	Displays the Call Home status.

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

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

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

Examples This example shows how to display the Call Home configuration information:

```
switch# show callhome
callhome disabled
Callhome Information:
contact person name(sysContact):who@where
contact person's email:
contact person's phone number:
street addr:
site id:
customer id:
contract id:ac12
switch priority:7
duplicate message throttling : enabled
periodic inventory : enabled
periodic inventory time-period : 7 days
periodic inventory timeofday : 08:00 (HH:MM)
Distribution : Disabled
switch#
```

Related Commands	Command	Description
	callhome	Configures a Call Home service.
	show callhome destination-profile	Displays Call Home information for a destination profile.

Send comments to nexus3k-docfeedback@cisco.com

show callhome destination-profile

To display the Call Home destination profile information, use the **show callhome destination-profile** command.

show callhome destination-profile [**profile** { **CiscoTAC-1** | *profile-name* | **full-txt-destination** | **short-txt-destination** }]

Syntax Description	profile	(Optional) Displays information about a specific destination profile.
	CiscoTAC-1	(Optional) Displays information for a CiscoTAC-1 destination profile.
	profile <i>profile-name</i>	(Optional) Displays information for a user-defined destination profile. The name can be a maximum of 32 alphanumeric characters.
	full-txt-destination	(Optional) Displays information of a destination profile configured for plain text messages.
	short-txt-destination	(Optional) Displays information of a destination profile configured for short text messages.

Command Default	All destination profiles
------------------------	--------------------------

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

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

Examples	This example shows how to display information about the Call Home destination profiles:
-----------------	---

```
switch# show callhome destination-profile
```

```
full_txt destination profile information
maximum message size:2500000
message format:full-txt
message-level:0
transport-method:email
email addresses configured:
```

```
url addresses configured:
```

```
alert groups configured:
all
```

```
short_txt destination profile information
maximum message size:4000
message format:short-txt
message-level:0
transport-method:email
<--Output truncated-->
switch#
```

Send comments to nexus3k-docfeedback@cisco.com

This example shows how to display information about a specific Call Home destination profile:

```
switch# show callhome destination-profile profile CiscoTAC-1
CiscoTAC-1 destination profile information
maximum message size:5000000
message-level:0
transport-method:email
email addresses configured:

url addresses configured:

alert groups configured:
cisco-tac

switch#
```

Related Commands

Command	Description
destination-profile	Creates a user-defined Call Home destination profile.
show callhome	Displays a summary of the Call Home configuration.

Send comments to nexus3k-docfeedback@cisco.com

show callhome transport-email

To display information about the e-mail configuration for Call Home, use the **show callhome transport-email** command.

show callhome transport-email

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

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

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

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

Examples	This example shows how to display the transport configuration for Call Home:
-----------------	--

```
switch# show callhome transport-email
from email addr:DCBU-5020-02@cisco.com
reply to email addr:junk@kunk.com
smtp server:192.168.1.236
smtp server port:25
switch#
```

Related Commands	Command	Description
	show callhome	Displays Call Home configuration information.
	show running-config callhome	Displays the running configuration information for Call Home.

Send comments to nexus3k-docfeedback@cisco.com

show callhome user-def-cmds

To display the user-defined CLI **show** commands added to a Call Home alert group, use the **show callhome user-def-cmds** command.

show callhome user-def-cmds

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

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

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

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

Examples	This example shows how to display the user-defined CLI show commands added to an alert group:
-----------------	--

```
switch# show callhome user-def-cmds
User configured commands for alert groups :
alert-group configuration user-def-cmd show running-config

switch#
```

Related Commands	Command	Description
	alert-group	Adds CLI show commands to a Call Home alert group.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the current bootup diagnostic level:</p> <pre>switch# show diagnostic bootup level</pre>
-----------------	---

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 nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the diagnostic results for a specific module:</p> <pre>switch# show diagnostic result module 1</pre>
----------	--

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 nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

show event manager environment

To display information about the configured environment variables, use the **show event manager environment** command.

show event manager environment {*variable-name* | **all**}

Syntax Description	<i>variable-name</i>	Name of the environment variable. The variable name can be any alphanumeric string up to 29 characters.
	all	Displays information about all the configured environment variables.

Defaults	None
-----------------	------

Command Modes	Any command mode
----------------------	------------------

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

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display information about the configured environment variables:
-----------------	---

```
switch# show event manager environment emailto
          emailto : admin@abc.com
switch#
```

Related Commands	Command	Description
	show event manager event-types	Displays information about the event manager event types.
	show event manager history events	Displays the history of events for all policies.
	show event manager policy-state	Displays information about a system policy.
	show event manager script system	Displays information about the script policies.
	show running-config eem	Displays information about running the configuration for the Embedded Event Manager (EEM).

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
show event manager system-policy	Displays information about the predefined system policies.
show startup-config eem	Displays information about the startup configuration for the Embedded Event Manager (EEM).

Send comments to nexus3k-docfeedback@cisco.com

show event manager event-types

To display information about the event manager event types, use the **show event manager event-types** command.

show event manager event-types *variable-name* | **all** | **module** [*slot*]

Syntax Description	<i>variable-name</i>	(Optional) Displays information about the specified event type.
	all	(Optional) Displays information about all the event types.
	module <i>slot</i>	(Optional) Displays information about the event types on other module. The range is from 1 to 1.
Defaults	None	
Command Modes	Any command mode	
Command History	Release	Modification
	5.0(3)U3(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	

Send comments to nexus3k-docfeedback@cisco.com

Examples

This example shows how to display information about the event manager event types:

```
switch# show event manager event-types all
Name : System_switchover
Description : switchover related events
Event Parameters : $vdc_no, $srv_name
Publisher : sysmgr
Default Action : collect information about sup state

Name : VDC_Events
Description : VDC create, delete and hap-reset events
Event Parameters : $vdc_no, $srv_name
Publisher : sysmgr
Default Action : collect information about sysmgr state in that vdc

Name : File_System_Events
Description : partition /dev/shm or /mnt/pss usage events
Event Parameters : $vdc_no, $srv_name
Publisher : sysmgr
Default Action : collect file system information

Name : Standby_Events
Description : gsync and vdc create events from standby
Event Parameters : $vdc_no, $srv_name
Publisher : sysmgr
Default Action : collect information about sysmgr state

Name : HAP_Reset
Description : HAP Reset in VDC
Event Parameters : $vdc_no, $srv_name
Publisher : sysmgr
Default Action : collect information about sysmgr state in that vdc

Name : Plugin_Events
Description : load Plugin related events
Event Parameters : $vdc_no, $srv_name
Publisher : sysmgr
Default Action : collect information about sysmgr state

Name : Service_Memory_Event
Description : Service Memory Usage Events. Action: Syslog
Event Parameters : majoralert, minoralert, clearalert, moduleno, vdc
Publisher : sysmgr
Default Action : None

Name : Switchover_Event
Description : Switchover count exceeded events
Event Parameters : swovercount, swoverthreshold
Publisher : sysmgr
Default Action : collect information about sysmgr state

Name : oir
Description : OIR event
Event Parameters : devicetype, eventtype, devicenum
Publisher : Platform Manager
Default Action : None

Name : fanabsent
Description : Fan Absent Event
Event Parameters : devicenum, time
Publisher : Platform Manager
Default Action : None

Name : fanbad
```

Send comments to nexus3k-docfeedback@cisco.com

Description : Fan Bad Event
 Event Parameters : devicenum, time
 Publisher : Platform Manager
 Default Action : None

Name : memory
 Description : Memory Alerts
 --More--
 switch(config)#

Related Commands

Command	Description
show event manager environment	Displays information about the configured environment variables.
show event manager history events	Displays the history of events for all policies.
show event manager policy-state	Displays information about a system policy.
show event manager script system	Displays information about the script policies.
show running-config eem	Displays information about the running configuration for the Embedded Event Manager (EEM).
show event manager system-policy	Displays information about the predefined system policies.
show startup-config eem	Displays information about the startup configuration for the Embedded Event Manager (EEM).

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

show event manager history events

To display the history of events for all policies, use the **show event manager history** command.

show event manager history events {**detail** [**maximum** *num-events* | **severity** [**catastrophic** | **minor** | **moderate** | **severe**]]}

Syntax Description		
detail	(Optional)	Displays information about all the event parameters.
maximum <i>num-events</i>	(Optional)	Specifies the maximum number of events to be displayed. The range is from 1 to 500.
severity	(Optional)	Displays the history of only those events whose severity is greater than or equal to the specified severity.
catastrophic	(Optional)	Displays the history of catastrophic events.
minor	(Optional)	Displays the history of minor events.
moderate	(Optional)	Displays the history of moderate events.
severe	(Optional)	Displays the history of severe events.

Defaults	None
-----------------	------

Command Modes	Any command mode
----------------------	------------------

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

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	<p>This example shows how to display the history of events for all policies:</p> <pre>switch# show event manager history events detail severity catastrophic switch#</pre>
-----------------	--

Related Commands	Command	Description
	show event manager environment	Displays information about the configured environment variables.
	show event manager event-types	Displays information about the event manager event types.
	show event manager policy-state	Displays information about a system policy.

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
show event manager script system	Displays information about the script policies.
show running-config eem	Displays information about the running configuration for the Embedded Event Manager (EEM).
show event manager system-policy	Displays information about the predefined system policies.
show startup-config eem	Displays information about the startup configuration for the Embedded Event Manager (EEM).

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

show event manager policy-state

To display information about a system policy, use the **show event manager policy-state** command.

show event manager policy-state *system-policy-name*

Syntax Description	<i>system-policy-name</i> Name of the internal system policy. The policy name can be any alphanumeric string up to 29 characters.
---------------------------	---

Defaults	None
-----------------	------

Command Modes	Any command mode
----------------------	------------------

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

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display information about a system policy:
	<pre>switch(config)# show event manager policy-state __pfm_fanabsent_any_singlefan Policy __pfm_fanabsent_any_singlefan Cfg count : 300 Hash Count Policy will trigger if ----- 0 10 290 more event(s) occur switch(config)#</pre>

Related Commands	Command	Description
	show event manager environment	Displays information about the configured environment variables.
	show event manager event-types	Displays information about the event manager event types.
	show event manager history events	Displays the history of events for all policies.
	show event manager script system	Displays information about the script policies.
	show running-config eem	Displays information about the running configuration for the Embedded Event Manager (EEM).

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
show event manager system-policy	Displays information about the predefined system policies.
show startup-config eem	Displays information about the startup configuration for the Embedded Event Manager (EEM).

Send comments to nexus3k-docfeedback@cisco.com

show event manager script system

To display information about the script policies, use the **show event manager script system** command.

show event manager script system *policy-name* | **all**

Syntax Description	<i>policy-name</i>	Name of the system script policy.
	all	Displays all the available system script policies.

Defaults	None
-----------------	------

Command Modes	Any command mode
----------------------	------------------

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

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display information about the script policies:
-----------------	--

```
switch# show event manager script system all
switch#
```

Related Commands	Command	Description
	show event manager environment	Displays information about the configured environment variables.
	show event manager event-types	Displays information about the event manager event types.
	show event manager history events	Displays the history of events for all policies.
	show event manager policy-state	Displays information about a system policy.
	show running-config eem	Displays information about the running configuration for the Embedded Event Manager (EEM).
	show event manager system-policy	Displays information about the predefined system policies.
	show startup-config eem	Displays information about the startup configuration for the Embedded Event Manager (EEM).

Send comments to nexus3k-docfeedback@cisco.com

show event manager system-policy

To display information about the predefined system policies, use the **show event manager system-policy** command.

show event manager system-policy *system-policy-name* | **all**

Syntax Description

system-policy-name Name of the system policy.

all Displays all policies including advanced and the policies that cannot be overridden.

Defaults

None

Command Modes

Any command mode

Command History

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

Usage Guidelines

This command does not require a license.

Send comments to nexus3k-docfeedback@cisco.com

Examples

This example shows how to display information about the predefined system policies:

```
switch# show event manager system-policy all
Name : __ethpm_debug_1
  Description : Action: none
  Overridable : Yes

      Name : __ethpm_debug_2
  Description : Action: none
  Overridable : Yes

      Name : __ethpm_debug_3
  Description : Action: none
  Overridable : Yes

      Name : __ethpm_debug_4
  Description : Action: none
  Overridable : Yes

      Name : __ethpm_link_flap
  Description : More than 30 link flaps in 420 seconds interval. Action: Error
Disable the port
  Overridable : Yes

      Name : __pfm_fanabsent_any_singlefan
  Description : Syslog when fan is absent
  Overridable : Yes

      Name : __pfm_fanbad_any_singlefan
  Description : Syslog when fan goes bad
  Overridable : Yes

      Name : __pfm_mem
  Description : Generate a syslog
  Overridable : No

      Name : __pfm_power_over_budget
  Description : Syslog warning for insufficient power overbudget
  Overridable : Yes

      Name : __pfm_tempev_major
  Description : TempSensor Major Threshold. Action: Shutdown
  Overridable : Yes

      Name : __pfm_tempev_minor
  Description : TempSensor Minor Threshold. Action: Syslog.
  Overridable : Yes

      Name : __sysmgr_not_active_six_sec
  Description : plugin load delay event. check sysmgr and plugin state
  Overridable : No

      Name : __sysmgr_policy_mem_alert
  Description : service memory usage event
  Overridable : Yes

      Name : __sysmgr_service_hap_reset
  Description : service hap reset event. check the services at fault and look
for the cores
  Overridable : No
--More--
switch#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	show event manager environment	Displays information about the configured environment variables.
	show event manager event-types	Displays information about the event manager event types.
	show event manager history events	Displays the history of events for all policies.
	show event manager policy-state	Displays information about a system policy.
	show event manager script system	Displays information about the script policies.
	show running-config eem	Displays information about the running configuration for the Embedded Event Manager (EEM).
	show startup-config eem	Displays information about the startup configuration for the Embedded Event Manager (EEM).

Send comments to nexus3k-docfeedback@cisco.com

show forwarding mpls stats

To display the MPLS statistics, use the **show forwarding mpls stats** command.

show forwarding mpls stats

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	6.0(2)U5(1)	This command was enhanced to display output statistics.
	6.0(2)U2(1)	This command was introduced.

Examples This example shows how to display the output statistics of a label. The output is now enhanced to display the output statistics. The output statistics is the sum of all egress adjacent statistics for a particular label.

```
switch# show forwarding mpls stats
Local |Prefix |FEC |Next-Hop |Interface |Out
Label |Table Id |(Prefix/Tunnel id) | |Label
3001 |0x80000001 |2000:1:255:201::1/128 |2000:1111:2121:1111:1111:1111:1 |Po21 |Pop
Label
HH: 100028, Refcount: 1
Input Pkts : 4372931 Input Bytes :559735168
Output Pkts: 4372936 Output Bytes:542244064
3002 |0x80000001 |2000:1:255:202::2/128 |2000:1111:2121:1111:1111:1111:1 |Po21 |Pop
Label
HH: 100026, Refcount: 1
Input Pkts : 4371209 Input Bytes :559514752
Output Pkts: 4371214 Output Bytes:542030536
3003 |0x80000001 |2000:1:255:203::3/128 |2000:1111:2121:1111:1111:1111:1 |Po21 |Pop
Label
HH: 100035, Refcount: 1
Input Pkts : 4372955 Input Bytes :559738240
Output Pkts: 4372959 Output Bytes:542246916
3000 |0x80000001 |2000:2000:2000:2000:2000:2000:2000/128
|2000:1111:2121:1111:1111:1111:1 |Po21 |Pop Label
HH: 100030, Refcount: 1
Input Pkts : 4371190 Input Bytes :559512320
Output Pkts: 4371195 Output Bytes:542028180
```


[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

show hardware forwarding memory health summary

To display the summary of parity error counts encountered for ASIC memory tables, use the **show hardware forwarding memory health summary** command.

show hardware forwarding memory health summary

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

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

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

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

Examples	This example shows how to display the summary of parity error counts encountered for ASIC memory tables:
-----------------	--

```
switch# show hardware forwarding memory health summary
Parity error counters:
Total parity error detections: 7
Total parity error corrections: 7
Total TCAM table parity error detections: 1
Total TCAM table parity error corrections: 1
Total SRAM table parity error detections: 6
Total SRAM table parity error corrections: 6
Parity error summary:
Table ID: L2 table      Detections: 1   Corrections: 1
Table ID: L3 Host table Detections: 1   Corrections: 1
Table ID: L3 LPM table  Detections: 1   Corrections: 1
Table ID: L3 LPM result table Detections: 1   Corrections: 1
Table ID: Ingress pre-lookup ACL result table Detections: 1   Corrections: 1
Table ID: Ingress ACL result table      Detections: 1   Corrections: 1
Table ID: Egress ACL result table        Detections: 1   Corrections: 1
```

Send comments to nexus3k-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)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the IP addresses of the DNS servers that are used to resolve hostnames:</p> <pre>switch# show hosts</pre>
-----------------	---

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

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the console logging configuration:</p> <pre>switch# show logging console</pre>
-----------------	---

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the logging configuration:</p> <pre>switch# show logging info</pre>
-----------------	---

Related Commands	Command	Description
	logging event	Logs interface events.

Send comments to nexus3k-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
	5.0(3)U1(1)	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 logfile	Configures the name of the log file used to store system messages.

Send comments to nexus3k-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.				
Command Default	None				
Command Modes	EXEC mode				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>5.0(3)U1(1)</td><td>This command was introduced.</td></tr> </table>	Release	Modification	5.0(3)U1(1)	This command was introduced.
Release	Modification				
5.0(3)U1(1)	This command was introduced.				

Examples

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

```
switch# show logging level
Facility           Default Severity      Current Session Severity
-----
aaa                 3                      3
aclmgr              3                      3
afm                 3                      3
altos               3                      3
auth                0                      0
authpriv            3                      3
bootvar             5                      5
callhome            2                      2
capability           2                      2
capability           2                      2
cdp                 2                      2
cert_enroll         2                      2
cfs                 3                      3
:
<--snip-->
:
vdc_mgr             6                      6
vlan_mgr            2                      2
vmm                 5                      5
vshd                5                      5
xmlma               3                      3
zschk               2                      2

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

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

Send comments to nexus3k-docfeedback@cisco.com

```
switch# show logging level port-channel
Facility          Default Severity    Current Session Severity
-----
eth_port_channel      5                      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 Address Resolution Protocol (ARP) logging severity level configuration:

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

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

switch#

Related Commands

Command	Description
logging level	Configures the facility logging level.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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 yyyy mmm dd hh:mm:ss	(Optional) Specifies a start time in the format yyyy mmm dd hh:mm:ss. Use three characters for the month (<i>mmm</i>) field, digits for the year (yyyy) and day (<i>dd</i>) fields, and digits separated by colons for the time (<i>hh:mm:ss</i>) field.
end-time yyyy mmm dd hh:mm:ss	(Optional) Specifies an end time in the format yyyy mmm dd hh:mm:ss. Use three characters for the month (<i>mmm</i>) field, digits for the year (yyyy) 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
5.0(3)U1(1)	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 nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the module logging configuration:</p> <pre>switch# show logging module</pre>
-----------------	--

Related Commands	Command	Description
	logging module	Configures module logging.

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the monitor logging configuration:</p> <pre>switch# show logging monitor</pre>
-----------------	---

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

Send comments to nexus3k-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	Release	Modification
	5.0(3)U1(1)	This command was introduced.

Examples	This example shows how to display the last 20 messages in the NVRAM log: switch# show logging nvram last 20
----------	---

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

Send comments to nexus3k-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 {bcm_used | boot-uptime | device-version | endtime |
environmental-history | exception-log | kernel-trace | obfl-history | obfl-logs | stack-trace |
starttime | status | trident} [> file || type]
```

Syntax Description

bcm_used	Displays the onboard failure logging (OBFL) BCM usage information.
boot-uptime	Displays the 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.
trident	Displays the OBFL Trident information.
> 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
7.0(3)I2(1)	While the induced errors are corrected on the switches, the log messages that notify the corrections stop after hitting a threshold (usually after 15 or 19 corrections). Also, an extra message gets printed when the parity error is injected.
5.0(3)U1(1)	This command was introduced.

Send comments to nexus3k-docfeedback@cisco.com

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:

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

The valid values for *type* are as follows:

- **begin [-i] [-x] [word]**—Begins 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.

Send comments to nexus3k-docfeedback@cisco.com

- **-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.
 - **-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.

Starting with Release 7.0(3)I2(1), while the induced errors are corrected on the switches, the log messages that notify the corrections stop after hitting a threshold (usually after 15 or 19 corrections). Also, an extra message gets printed when the parity error is injected.

Examples

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

```
switch# show logging onboard boot-uptime
```

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

```
switch# show logging onboard 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.

Send comments to nexus3k-docfeedback@cisco.com

- 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
- 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 nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	This example shows how to display the pending changes to the syslog server configuration: switch# show logging pending
-----------------	--

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

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the pending differences of the syslog server configuration:</p> <pre>switch# show logging pending-diff</pre>
-----------------	---

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

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the logging session status:</p> <pre>switch# show logging session status</pre>
-----------------	---

Related Commands	Command	Description
	logging timestamp	Sets the logging time-stamp units.

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the syslog server configuration:</p> <pre>switch# show logging server</pre>
-----------------	--

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
----------------------	-----------

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

Examples	<p>This example shows how to display the logging status:</p> <pre>switch# show logging status</pre>
-----------------	--

Related Commands	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 nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the logging time-stamp configuration:</p> <pre>switch# show logging timestamp</pre>
-----------------	--

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

Send comments to nexus3k-docfeedback@cisco.com

show monitor session

To display information about the Switched Port Analyzer (SPAN) or Encapsulated Remote Switched Port Analyzer (ERSPAN) sessions, use the **show monitor session** command.



Note Beginning with Release 7.0(3)I2(1), the rx, tx, and both options are displayed for the source VLANs and an option for the filter VLANs is not displayed. Also, the number of TCAM entries available for ACL SPAN has been reduced by 6 entries.

show monitor session [*session* | **all** [**brief**] | **range** *range* [**brief**]]

Syntax Description

<i>session</i>	(Optional) Number of the session. The range is from 1 to 18.
all	(Optional) Displays all sessions.
brief	(Optional) Displays a brief summary of the information.
range <i>range</i>	(Optional) Displays a range of sessions. The range is from 1 to 18.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.0(3)U1(1)	This command was introduced.
5.0(3)U2(2)	Support for ERSPAN was added.
6.0(2)U5(1)	The egress interface information is added for the ERSPAN source session.
7.0(3)I2(1)	This command displays rx , tx , and both options for the source VLANs and does not display an option for the filter VLANs

Examples

This example shows how to display information about SPAN session 1:

```
switch# show monitor session 1
session 1
-----
type : erspan-source
state : up
vrf-name : default
destination-ip : 90.1.1.1
ip-ttl : 255
ip-dscp : 0
acl-name : acl-name not specified
origin-ip : 200.1.1.1 (global)
source intf :
rx : Eth1/9
tx : Eth1/9
both : Eth1/9
source VLANs :
```

Send comments to nexus3k-docfeedback@cisco.com

```
filter VLANs : filter not specified
rx :
source fwd drops :
egress-intf : Po10switch
switch#
```

This example shows the information displayed beginning with release 7.0(3)I2(1).

```
switch# show monitor session 1
session 1
-----
type : local
state : down (Session admin shut)
acl-name : acl-name not specified
source intf :
rx :
tx :
both :
source VLANs :
rx : 5
tx :
both :
filter VLANs : filter not specified
source fwd drops :
destination ports :
switch#
```

This example shows how to display a range of SPAN sessions:

```
switch# show monitor session range 1-4
```

This example shows how to display the information about an ERSPAN session on a switch that runs Cisco NX-OS Release 5.0(3)U2(2):

```
switch# show monitor session 1
session 1
-----
type : erspan-source
state : up
vrf-name : default
destination-ip : 90.1.1.1
ip-ttl : 255
ip-dscp : 0
acl-name : acl-name not specified
origin-ip : 200.1.1.1 (global)
source intf :
rx : Eth1/9
tx : Eth1/9
both : Eth1/9
source VLANs :
filter VLANs : filter not specified
rx :
source fwd drops :
egress-intf : Po10switch
switch#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	monitor session	Displays the contents of the startup configuration file.
	show running-config monitor	Displays the running configuration information for SPAN and ERSPAN sessions.

Send comments to nexus3k-docfeedback@cisco.com

show mpls strip labels

To display the MPLS label configuration, use the **show mpls strip labels** command.

show mpls strip labels [*label* | **all** | **dynamic** | **static**]

Syntax Description	<i>label</i>	Specifies the label to be displayed.
	all	Specifies that all labels must be displayed. This is the default option.
	dynamic	Specifies that only dynamic labels must be displayed.
	static	Specifies that only static labels must be displayed.

Command Default All labels are displayed.

Command Modes EXEC mode

Command History	Release	Modification
	6.0(2)U2(5)	This command was introduced.

Examples This example shows how to display all MPLS labels:

```
switch(config)# show mpls strip labels
```

```
MPLS Strip Labels:
```

```
Total      : 3005
```

```
Static      : 5
```

```
Legend:      * - Static Label
```

```
Interface - where label was first learned
```

```
Idle-Age   - Seconds since last use
```

```
SW-Counter- Packets received in Software
```

```
HW-Counter- Packets switched in
```

```
Hardware-----
```

	Label	Interface	Idle-Age	SW-Counter	HW-Counter
	4096	Eth1/53/1	15	1	210
	4097	Eth1/53/1	15	1	210
	4098	Eth1/53/1	15	1	210
	4099	Eth1/53/1	7	2	219
	4100	Eth1/53/1	7	2	219
	4101	Eth1/53/1	7	2	219
	4102	Eth1/53/1	39	1	206
	4103	Eth1/53/1	39	1	206
	4104	Eth1/53/1	39	1	206
	4105	Eth1/53/1	1	1	217
	4106	Eth1/53/1	1	1	217
	4107	Eth1/53/1	1	1	217
	4108	Eth1/53/1	15	1	210
*	25000	None <User>	39	1	206
*	20000	None <User>	39	1	206
*	21000	None <User>	1	1	217

Send comments to nexus3k-docfeedback@cisco.com

This example shows how to display only static MPLS labels:

```
switch(config)# show mpls strip labels static
```

```
MPLS Strip Labels:
```

```
Total      : 3005
```

```
Static      : 5
```

```
Legend:      * - Static Label
```

```
Interface - where label was first learned
```

```
Idle-Age   - Seconds since last use
```

```
SW-Counter- Packets received in Software
```

```
HW-Counter- Packets switched in Hardware
```

	Label	Interface	Idle-Age	SW-Counter	HW-Counter
*	300	None <User>	403	0	0
*	100	None <User>	416	0	0
*	25000	None <User>	869	0	0
*	20000	None <User>	869	0	0
*	21000	None <User>	869	0	0

Related Commands

Command	Description
mpls strip	Enables the MPLS stripping feature.
mpls strip dest-mac	Configures the destination MAC address for stripped egress frames.
mpls strip label	Adds or deletes static MPLS labels.
mpls strip label-age	Configures MPLS label aging.
clear mpls strip label dynamic	Clears dynamic label entries.

Send comments to nexus3k-docfeedback@cisco.com

show ntp access-groups

To display the Network Time Protocol (NTP) access group configuration, use the **show ntp access-groups** command.

show ntp access-groups

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes EXEC mode

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to display the NTP access group configuration:

```
switch# show ntp access-groups
-----
Access List                               Type
-----
Admin_Group_123                           Peer
switch#
```

Related Commands	Command	Description
	ntp access-group peer	Configures an NTP access group.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

show ntp authentication-keys

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

show ntp authentication-keys

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

Defaults	None
-----------------	------

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

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display the NTP authentication keys:
-----------------	--

```
switch# show ntp authentication-keys
-----
Auth key      MD5 String
-----
3             cisco
42            Nice_Key
34567         nexus7k
switch#
```

Related Commands	Command	Description
	show ntp authentication-status	Displays the status of all NTP authentication.
	ntp authentication-key	Configures one or more keys that a time source must provide in its NTP packets in order for the device to synchronize to it.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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.
---------------------------	--

Defaults	None
-----------------	------

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

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display the NTP authentication status:
-----------------	--

<pre>switch# show ntp authentication-status Authentication enabled. switch#</pre>

Related Commands	Command	Description
	ntp authenticate	Enables NTP authentication.
	show ntp authentication-keys	Displays the configured NTP authentication keys.

Send comments to nexus3k-docfeedback@cisco.com

show ntp logging-status

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

show ntp logging-status

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

Defaults	None
-----------------	------

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

Command History	Release	Modification
	6.0(2)U(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display the NTP logging status:
-----------------	---

```
switch# show ntp logging-status
NTP logging enabled.
switch#
```

Related Commands	Command	Description
	ntp logging	Enables NTP logging.
	show ntp authentication-status	Displays the status of NTP authentication.
	show ntp session status	Displays the NTP distribution session information.

Send comments to nexus3k-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
	6.0(2)U2(1)	This command was introduced.

Examples	<p>This example shows how to display information about NTP peers:</p> <pre>switch# show ntp peers</pre>
-----------------	--

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
	6.0(2)U2(1)	This command was introduced.

Examples	<p>This example shows how to display the peer status for NTP:</p> <pre>switch# show ntp peer-status</pre>
-----------------	---

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

Send comments to nexus3k-docfeedback@cisco.com

show ntp pending-diff

To display the differences between the pending Network Time Protocol (NTP) configuration and the active NTP configuration, use the **show ntp pending-diff** command.

show ntp pending-diff

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

Defaults	None
-----------------	------

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

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display the differences between the pending NTP configuration and the active NTP configuration:
-----------------	---

```
switch# show ntp pending-diff
switch#
```

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

show ntp pending peers

To display pending Network Time Protocol (NTP) configuration changes on all peers, use the **show ntp pending peers** command.

show ntp pending peers

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

Defaults	None
-----------------	------

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

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display the pending NTP configuration changes on all peers:
-----------------	---

switch# show ntp pending peers
switch#

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

Send comments to nexus3k-docfeedback@cisco.com

show ntp session status

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

show ntp session status

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

Defaults	None
-----------------	------

Command Modes	Any command mode
----------------------	------------------

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display the NTP session status:
-----------------	---

```
switch# show ntp session status
Last Action Time Stamp      : Thu Aug 1 16:22:00 20
Last Action                  : Distribution Enable
Last Action Result           : Success
Last Action Failure Reason   : none
switch#
```

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

show ntp status

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

show ntp status

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

Defaults	None
-----------------	------

Command Modes	Any command mode
----------------------	------------------

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display the NTP distribution status:
-----------------	--

```
switch(config)# show ntp status
Distribution : Disabled
Last operational state: No session
switch(config)#
```

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

Send comments to nexus3k-docfeedback@cisco.com

show ntp source

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

show ntp source

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

Defaults	None
-----------------	------

Command Modes	Any command mode
----------------------	------------------

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display the NTP source information: <pre>switch(config)# show ntp source</pre>
-----------------	---

Related Commands	Command	Description
	ntp source	Configures the NTP source.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

show ntp source-interface

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

show ntp source-interface

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

Defaults	None
-----------------	------

Command Modes	Any command mode
----------------------	------------------

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display the NTP source interface:
-----------------	---

```
switch(config)# show ntp source-interface
Source interface loopback1
switch(config)#
```

Related Commands	Command	Description
	show startup-config ntp	Displays information about the startup NTP configuration of the switch.
	show running-config ntp	Displays information about the NTP configuration that is currently running on the switch.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	This example shows how to display the statistics for NTP:
	switch# show ntp statistics local

Related Commands	Command	Description
	clear ntp statistics	Clears NTP statistics

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

show ntp status

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

show ntp status

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Any command mode

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to display the distribution status for NTP.

```
switch(config)# show ntp status
Distribution : Enabled
Last operational state: No session
```


Send comments to nexus3k-docfeedback@cisco.com

show ntp trusted-keys

To display the configured Network Time Protocol (NTP) trusted keys, use the **show ntp trusted-keys** command.

show ntp trusted-keys

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

Defaults	None
-----------------	------

Command Modes	Any command mode
----------------------	------------------

Command History	Release	Modification
	6.0(2)U(2)1	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display all the configured NTP trusted keys:
-----------------	--

```
switch(config)# show ntp trusted-keys
Trusted Keys:
42
switch(config)#
```

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

show ptp brief

Command	Description
ntp trusted-keys	Displays the configured NTP authentication keys.
To display a brief status of the Precision Time Protocol (PTP) interfaces, use the show ptp brief command.	

show ptp brief

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to display a brief status of the PTP interfaces:

```
switch# show ptp brief

PTP port status
-----
Port          State
-----
Eth1/5        Disabled
switch#
```

Related Commands	Command	Description
	show ptp clock	Displays the properties of the local clock.
	show ptp clock 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.
	show ptp port	Displays the status of the PTP port.
	show ptp time-property	Displays the properties of the PTP clock.

Send comments to nexus3k-docfeedback@cisco.com

show ptp clock

To display the Precision Time Protocol (PTP) clock information, use the **show ptp clock** command.

show ptp clock

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

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

Command Modes	Any command mode
----------------------	------------------

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display the PTP clock information:
-----------------	--

```
switch# show ptp clock
PTP Device Type: Boundary clock
Clock Identity : 54:7f:ee:ff:ff: 2:47:81
Clock Domain: 1
Number of PTP ports: 0
Priority1 : 255
Priority2 : 255
Clock Quality:
    Class : 248
    Accuracy : 254
    Offset (log variance) : 65535
Offset From Master : 0
Mean Path Delay : 0
Steps removed : 0
Local clock time:Fri Sep 30 05:57:50 2011
switch#
```

Related Commands	Command	Description
	show ptp brief	Displays the PTP status.
	show ptp clock 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.

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
show ptp port	Displays the status of the PTP port.
show ptp time-property	Displays the properties of the PTP clock.

Send comments to nexus3k-docfeedback@cisco.com

show ptp clock foreign-masters-record

To display information about the state of foreign masters known to the Precision Time Protocol (PTP) process, use the **show ptp clock foreign-masters-record** command.

show ptp clock foreign-masters-record [**interface ethernet** *slot/port*]

Syntax Description	interface	(Optional) Specifies an interface.
	ethernet	Specifies an IEEE 802.3z Ethernet interface.
	<i>slot/port</i>	Slot number of the Ethernet interface. The slot number is from 1 to 255 and the port number is form 1 to 128.

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

Command Modes	Any command mode
----------------------	------------------

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display information about the state of foreign masters known to the PTP process:
-----------------	--

```
switch# show ptp clock foreign-masters-record
```

This example shows how to display information about the state of foreign masters known to the PTP process for the Ethernet interface 1/5:

```
switch# show ptp clock foreign-masters-record interface ethernet 1/5
```

Send comments to nexus3k-docfeedback@cisco.com

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 parent	Displays the properties of the PTP parent.
	show ptp port	Displays the status of the PTP port.
	show ptp time-property	Displays the properties of the PTP clock.

Send comments to nexus3k-docfeedback@cisco.com

show ptp corrections

To display the history of the Precision Time Protocol (PTP) clock corrections on the Ethernet interfaces, use the **show ptp corrections** command.

show ptp corrections

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

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

Command Modes	Any command mode
----------------------	------------------

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display the history of the PTP clock corrections on the Ethernet interfaces: <pre>switch# show ptp corrections</pre>
-----------------	---

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

show ptp parent

To display information about the parent and grand master of the Precision Time Protocol (PTP) clock, use the **show ptp parent** command.

show ptp parent

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

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

Command Modes	Any command mode
----------------------	------------------

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display information about the parent and grand master of the PTP clock:
-----------------	---

```
switch# show ptp parent
```

```
PTP PARENT PROPERTIES
```

```
Parent Clock:
```

```
Parent Clock Identity:  0: 0: 0:ff:ff: 0: 0: 0
```

```
Parent Port Number: 0
```

```
Observed Parent Offset (log variance): N/A
```

```
Observed Parent Clock Phase Change Rate: N/A
```

```
Grandmaster Clock:
```

```
Grandmaster Clock Identity:  0: 0: 0:ff:ff: 0: 0: 0
```

```
Grandmaster Clock Quality:
```

```
    Class: 248
```

```
    Accuracy: 254
```

```
    Offset (log variance): 65535
```

```
    Priority1: 255
```

```
    Priority2: 255
```

```
switch#
```


Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	show ptp brief	Displays the PTP status.
	show ptp clock	Displays the properties of the local clock.
	show ptp clock 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	Displays the status of the PTP port.
	show ptp time-property	Displays the properties of the PTP clock.

Send comments to nexus3k-docfeedback@cisco.com

show ptp port

To display information about the Precision Time Protocol (PTP) port, use the **show ptp port** command.

show ptp port interface ethernet *slot/port*

Syntax Description	interface	Specifies the interface.
	ethernet <i>slot/port</i>	Specifies an IEEE 802.3z Ethernet interface. The slot number is from 1 to 255 and the port number is from 1 to 128.

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

Command Modes	Any command mode
---------------	------------------

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines	This command does not require a license.
------------------	--

Examples	This example shows how to display information about the PTP port on the Ethernet interface 1/5:
----------	---

```
switch# show ptp port interface ethernet 1/5
PTP Port Dataset: Eth1/5
Port identity: clock identity: 0: 5:73:ff:ff:ff:5b: 1
Port identity: port number: 4
PTP version: 2
Port state: Disabled
VLAN info: 1
Delay request interval(log mean): 2
Peer mean path delay: 0
Announce interval(log mean): 1
Sync interval(log mean): -2
Delay Mechanism: End to End
Peer delay request interval(log mean): 0
switch#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	show ptp brief	Displays the PTP status.
	show ptp clock	Displays the properties of the local clock.
	show ptp clock 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.
	show ptp time-property	Displays the properties of the PTP clock.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

show ptp time-property

To display the Precision Time Protocol (PTP) clock properties, use the **show ptp time-property** command.

show ptp time-property

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

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

Command Modes	Any command mode
----------------------	------------------

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

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

```
switch# show ptp time-property
PTP CLOCK TIME PROPERTY:
    Current UTC Offset valid: 0
    Current UTC Offset: 0
    Leap59: 0
    Leap61: 0
    Time Traceable: 0
    Frequency Traceable: 0
    PTP Timescale: 0
    Time Source: 0xa0(Internal Oscillator)
switch#
```

Related Commands	Command	Description
	show ptp brief	Displays the PTP status.
	show ptp clock	Displays the properties of the local clock.
	show ptp clock 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.
	show ptp port	Displays the status of the PTP port.

Send comments to nexus3k-docfeedback@cisco.com

show rmon

To display information about Remote Monitoring (RMON) alarms or high-capacity alarms or events, use the **show rmon** command.

show rmon {alarms | events | hcalarms | info | logs}

Syntax Description	alarms	Displays the RMON alarms.
	events	Displays the RMON events.
	hcalarms	Displays the RMON high-capacity alarms.
	info	Displays the RMON configuration information.
	logs	Displays information about the RMON event logs.

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

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

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

Examples This example shows how to display the RMON high-capacity alarms configured on the switch:

```
switch# show rmon hcalarms
High Capacity Alarm 3 is active, owned by admin
Monitors 1.3.6.1.2.1.2.2.1.17.83886080 every 5 second(s)
Taking delta samples, last value was 216340
Rising threshold is 0, assigned to event 3
Falling threshold is 0, assigned to event 0
On startup enable rising alarm
Number of Failed Attempts is 0
switch#
```

This example shows how to display the RMON events configured on the switch:

```
switch# show rmon events
Event 5 is active, owned by admin
Description is myRMONEvent
Event firing causes nothing, last fired never
switch#
```

This example shows how to display the RMON configuration information:

```
switch# show rmon info
Maximum allowed 32 bit or 64 bit alarms : 512
Number of 32 bit alarms configured : 0
Number of 64 bit hcalarms configured : 1
switch#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	rmon alarm	Creates RMON alarms.
	rmon event	Creates RMON events.
	rmon hcalarm	Creates RMON high-capacity alarms.
	show running-config	Displays the running configuration.

Send comments to nexus3k-docfeedback@cisco.com

show running-config

To display the contents of the currently running configuration file, use the **show running-config** command.

show running-config [all]

Syntax Description	all (Optional) Displays the full operating information including default settings.
--------------------	---

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

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

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

Examples This example shows how to display information on the running configuration on a switch that runs Cisco NX-OS Release 5.0(3)U1(1):

```
switch# show running-config

!Command: show running-config
!Time: Fri May 28 10:30:02 2010

version 5.0(3)U1(1)
feature telnet
feature private-vlan

username adminbackup password 5 ! role network-operator
username admin password 5 $1$gLP0Z4.z$N4fMnTcHmdSgQ3ENakm/1 role network-admin
ip domain-lookup
hostname switch
slot 1
snmp-server user admin network-admin auth md5 0xd727e3e4ed39de2f32841ffa24e4234c
priv 0xd727e3e4ed39de2f32841ffa24e4234c localizedkey

vrf context management
ip route 0.0.0.0/0 192.168.0.1
<--Output truncated-->
switch#
```

This example shows how to display detailed information on the running configuration on a switch that runs Cisco NX-OS Release 5.0(3)U1(1):

```
switch# show running-config all
```

Send comments to nexus3k-docfeedback@cisco.com

This example shows how to display the running configuration on a switch that runs Cisco NX-OS Release 5.0(3)U2(1) and shows the Control Plane Policing (CoPP) policy maps, hardware port modes, and access control list (ACL) ternary content addressable memory (TCAM) changes:

```
switch# show running-config

!Command: show running-config
!Time: Thu Aug 25 07:39:37 2011

version 5.0(3)U2(1)
feature telnet
no feature ssh
feature lldp

username admin password 5 $1$OOV4MdOM$BAB5RkD22YanT4empqqSM0 role network-admin
ip domain-lookup
switchname switch
ip access-list my-acl
  10 deny ip any 10.0.0.1/32
  20 deny ip 10.1.1.1/32 any
class-map type control-plane match-any copp-arp
class-map type control-plane match-any copp-bpdu
class-map type control-plane match-any copp-default
class-map type control-plane match-any copp-dhcp
class-map type control-plane match-any copp-filtermatch
class-map type control-plane match-any copp-icmp
:
<--snip-->
:
class-map type control-plane match-any copp-ttl1
policy-map type control-plane copp-system-policy
  class copp-default
    police pps 400
  class copp-l2switched
    police pps 400
  class copp-icmp
    police pps 200
:
<--snip-->
control-plane
  service-policy input copp-system-policy
hardware profile tcam region arpacl 128
hardware profile tcam region ifacl 256
hardware profile tcam region racl 256
hardware profile tcam region vacl 512
hardware profile portmode 48x10G+4x40G
<--Output truncated-->
switch#
```

Related Commands

Command	Description
show startup-config	Displays the contents of the startup configuration file.

Send comments to nexus3k-docfeedback@cisco.com

show running-config callhome

To display the Call Home running configuration, use the **show running-config callhome** command.

show running-config callhome [all]

Syntax Description	all (Optional) Displays all the default and configured information.
--------------------	--

Command Default	Displays only the configured information.
-----------------	---

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

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

Examples	<p>This example shows how to display the Call Home running configuration:</p> <pre>switch# show running-config callhome</pre> <p>This example shows how to display the entire Call Home running configuration, including the default values:</p> <pre>switch# show running-config callhome all</pre>
----------	--

Related Commands	Command	Description
	show callhome	Displays Call Home configuration information.

Send comments to nexus3k-docfeedback@cisco.com

show running-config eem

To display information about running configuration for the Embedded Event Manager (EEM), use the **show running-config eem** command.

show running-config eem

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

Defaults	None
-----------------	------

Command Modes	Any command mode
----------------------	------------------

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

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display information about running configuration for the EEM:
-----------------	--

```
switch # show running-config eem

!Command: show running-config eem
!Time: Thu Feb 23 01:53:06 2012

version 5.0(3)U5(1)
event manager environment emailto "admin@abc.com"
event manager applet default-applet
  action 1.1 cli show version
"
  action 1.2 counter name count1 value $variable op dec
event manager applet eventcli-applet
  event oir fan remove 1
event manager applet monitorShutdown
  description "Monitors interface shutdown."
  event cli match "shutdown"
  action 1.0 cli show interface ethernet 3/1
event manager applet snmp-applet
  event snmp oid 4.2.1.6 get-type next entry-op eq entry-val 42 poll-interval 32
1321321
  action 1.7 snmp-trap strdata "EEM detected server failure"
event manager applet syslog-applet
  action 1.7 syslog priority critical msg cpu usage high
event manager applet test_app
event manager applet tracking-applet
  event track 20 state up

switch#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	show event manager environment	Displays information about the configured environment variables.
	show event manager event-types	Displays information about the event manager event types.
	show event manager history events	Displays the history of events for all policies.
	show event manager policy-state	Displays information about a system policy.
	show event manager script system	Displays information about the script policies.
	show event manager system-policy	Displays information about the predefined system policies.
	show startup-config eem	Displays information about the startup configuration for the Embedded Event Manager (EEM).

Send comments to nexus3k-docfeedback@cisco.com

show running-config exclude-provision

To display the running configuration without the configuration for offline preprovisioned interfaces, use the **show running-config exclude-provision** command.

show running-config exclude-provision

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

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

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

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

Examples	This example shows how to display the running configuration without the offline preprovisioned interfaces:
-----------------	--

```
switch# show running-config exclude-provision

!Command: show running-config exclude-provision
!Time: Fri May 28 10:35:32 2010

version 5.0(3)U1(1)
feature telnet
feature private-vlan

username adminbackup password 5 ! role network-operator
username admin password 5 $1$gLP0Z4.z$N4fMnTcHmdSgQ3ENakm/1 role network-admin
ip domain-lookup
hostname switch
slot 1
snmp-server user admin network-admin auth md5 0xd727e3e4ed39de2f32841ffa24e4234c
priv 0xd727e3e4ed39de2f32841ffa24e4234c localizedkey

vrf context management
ip route 0.0.0.0/0 192.168.0.1
vlan 1
vlan 5
private-vlan primary
port-channel load-balance ethernet source-ip

interface Ethernet1/1
<--Output truncated-->
switch#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	copy running-config startup-config	Copies the running configuration to the startup configuration.
	provision	Preprovisions a module in a slot.
	show provision	Displays the preprovisioned module information.
	show startup-config exclude-provision	Displays the startup configuration without the preprovisioning information for offline interfaces.
	slot	Configures a chassis slot for a predefined module.

Send comments to nexus3k-docfeedback@cisco.com

show running-config interface

To display the running configuration information for interfaces, use the **show running-config interface** command.

show running-config interface [**all** | **ethernet** *slot/port* | **loopback** *if_number* | **mgmt** *mgmt_intf* | **port-channel** *po_number*]

Syntax Description		
all		(Optional) Displays all the default and configured information.
ethernet <i>slot/port</i>		Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback <i>if_number</i>		Specifies the loopback interface. The loopback interface number is from 0 to 1023.
mgmt <i>mgmt_intf</i>		Specifies the management interface. The interface number is 0.
port-channel <i>number</i>		Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.

Command Default	Displays only the configured information.
------------------------	---

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

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

Examples This example shows how to display the running configuration for a specified Ethernet interface on a switch that runs Cisco NX-OS Release 5.0(3)U2(1):

```
switch# show running-config interface ethernet 1/5

!Command: show running-config interface Ethernet1/5
!Time: Fri Aug 26 04:12:01 2011

version 5.0(3)U2(1)

interface Ethernet1/5
  speed auto

switch#
```

Related Commands	Command	Description
	copy running-config startup-config	Copies the running configuration information to the startup configuration file.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

show running-config monitor

To display the running configuration for the Switched Port Analyzer (SPAN) or Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **show running-config monitor** command.

show running-config monitor [all]

Syntax Description	all	(Optional) Displays current SPAN configuration information including default settings.
Command Default	None	
Command Modes	EXEC mode	
Command History	Release	Modification
	5.0(3)U1(1)	This command was introduced.
	5.0(3)U2(2)	Support for ERSPAN was added.

Examples

This example shows how to display information on the running SPAN and ERSPAN configuration:

```
switch# show running-config monitor

!Command: show running-config monitor
!Time: Wed Sep 28 19:11:41 2011

version 5.0(3)U2(2)
monitor session 1 type erspan-source
  description ERSPAN source session
  vrf default
  destination ip 192.0.2.1
  ip ttl 5
  ip dscp 3
  source interface Ethernet1/5 both
  mtu 1000
  no shut
monitor session 3 type erspan-destination
  description ERSPAN destination session
  source ip 192.0.1.1
  destination interface Ethernet1/2

switch#
```

This example shows how to display detailed information on the running SPAN and ERSPAN configuration:

```
switch# show running-config monitor all
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	monitor session	Configures SPAN or ERSPAN sessions.
	show monitor session	Displays information about SPAN or ERSPAN sessions.

Send comments to nexus3k-docfeedback@cisco.com

show running-config ptp

To display the Precision Time Protocol (PTP) running configuration, use the **show running-config ptp** command.

show running-config ptp [all]

Syntax Description	all (Optional) Displays all the default and configured information.
---------------------------	--

Command Default	Displays only the configured information.
------------------------	---

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

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

Examples

This example shows how to display the PTP running configuration:

```
switch# show running-config ptp

!Command: show running-config ptp
!Time: Wed Aug 24 08:09:22 2011

version 5.0(3)U2(2)
feature ptp


ptp domain 1
ptp source 192.0.2.1
ptp priority1 10
ptp priority2 20

interface Ethernet1/5
  ptp
  ptp vlan 5
  ptp delay-request minimum interval 2

switch#
```

This example shows how to display the entire PTP running configuration, including the default values:

```
switch# show running-config ptp all
```

 show running-config ptp

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	copy running-config startup-config	Copies the PTP running configuration information to the startup configuration file.
	show startup-config ptp	Displays the startup configuration information.

Send comments to nexus3k-docfeedback@cisco.com

show scheduler

To display information about the scheduled maintenance jobs, use the **show scheduler** command.

```
show scheduler { config | internal [mem-stats] | job [name jobname] | logfile | schedule [name schedulename]}
```

Syntax Description	config	Displays the scheduler configuration information.
	internal	Provides the internal scheduler information as specified.
	mem-stats	(Optional) Provides the scheduler internal memory information as specified.
	job	Displays the job information as specified.
	name jobname	(Optional) Displays information for the specified scheduler job name. The job name can be any alphanumeric string up to 31 characters.
	logfile	Displays the scheduler log file as specified.
	schedule	Displays the scheduler timetable as specified.
	name schedulename	(Optional) Displays the scheduler timetable for the specified schedule name. The schedule name can be any alphanumeric string up to 31 characters.

Defaults	None
----------	------

Command Modes	Any command mode
---------------	------------------

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

Usage Guidelines	This command does not require a license.
------------------	--

Examples	<p>This example shows how to display the scheduler configuration:</p> <pre>switch# show scheduler config config terminal feature scheduler scheduler logfile size 16 end switch#</pre>
----------	---

Related Commands

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
scheduler	Configures maintenance jobs.
feature scheduler	Enables the scheduler feature for scheduling maintenance jobs.

Send comments to nexus3k-docfeedback@cisco.com

show sflow

To display information about the sFlow global configuration, use the **show sflow** command.

show sflow

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

Defaults	None
-----------------	------

Command Modes	Global command mode.
----------------------	----------------------

Command History	Release	Modification
	5.0(3)U4(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to configure sFlow information:
-----------------	--

```
switch(config)# feature sflow
switch(config)# sflow sampling-rate 5000
switch(config)# sflow max-sampled-size 200
switch(config)# sflow counter-poll-interval 100
switch(config)# sflow max-datagram-size 2000
switch(config)# sflow collector-ip 192.0.2. vrf management
switch(config)# sflow collector-port 7000
switch(config)# sflow agent-ip 192.0.2.3
switch(config)# sflow data-source interface ethernet 1/5
```

Related Commands	Command	Description
	feature sflow	Enables sFlow.

Send comments to nexus3k-docfeedback@cisco.com

show sflow statistics

To display the sFlow statistics, use the **show sflow statistics** command.

show sflow statistics

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

Defaults	None
-----------------	------

Command Modes	Global command mode.
----------------------	----------------------

Command History	Release	Modification
	5.0(3)U4(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to configure sFlow information:
-----------------	--

```
switch(config)# feature sflow statistics
```

```
Total Packets      : 7157396604
Total Samples      : 40759311
Processed Samples   : 40759347
Dropped Samples     : 0
Sent Datagrams      : 6823652
Dropped Datagrams   : 4
```

```
#####
```

Related Commands	Command	Description
	feature sflow	Enables sFlow.
	show sflow	Displays the sFlow global configuration.

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the SNMP community strings:</p> <pre>switch# show snmp community</pre>
-----------------	---

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
	5.0(3)U1(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 nexus3k-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
	5.0(3)U1(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
-----------------	--

Related Commands	Command	Description
	show running-config	Displays the running system configuration information.
	snmp-server user	Configures a new user to a SNMP group.

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	This example shows how to display the SNMP groups:
	switch# show snmp group

Related Commands	Command	Description
	show running-config	Displays the running system configuration information.

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the SNMP host:</p> <pre>switch# show snmp host</pre>
-----------------	---

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
	5.0(3)U1(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	Displays the running system configuration information.

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	<p>This example shows how to display the SNMP traps:</p> <pre>switch# show snmp trap</pre>
-----------------	--

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	This example shows how to display the SNMP users configured on the switch:
-----------------	--

```
switch# show snmp user
```

This example shows how to display information about a specific SNMP user:

```
switch# show snmp user admin
```

Related Commands	Command	Description
	snmp-server user	Configures a new user to an SNMP group.

Send comments to nexus3k-docfeedback@cisco.com

show startup-config

To display the contents of the currently running configuration file, use the **show startup-config** command.

show startup-config

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

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

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

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

Examples	This example shows how to display information from the startup configuration file:
-----------------	--

```
switch# show startup-config

!Command: show startup-config
!Time: Fri May 28 11:05:41 2010
!Startup config saved at: Fri May 28 11:05:35 2010

version 5.0(3)U1(1)
feature telnet
feature private-vlan

username adminbackup password 5 ! role network-operator
username admin password 5 $1$gLP0Z4.z$nA4fMnTcHmdSgQ3ENakm/1 role network-admin
ip domain-lookup
hostname switch
slot 1
snmp-server user admin network-admin auth md5 0xd727e3e4ed39de2f32841ffa24e4234c
priv 0xd727e3e4ed39de2f32841ffa24e4234c localizedkey
<---Output truncated-->
switch#
```

Related Commands	Command	Description
	show running-config	Displays the contents of the currently running configuration file.

Send comments to nexus3k-docfeedback@cisco.com

show startup-config callhome

To display the startup configuration for Call Home, use the **show startup-config callhome** command.

show startup-config callhome

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

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

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

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

Examples	<p>This example shows how to display the startup configuration for Call Home:</p> <pre>switch# show startup-config callhome</pre>
-----------------	---

Related Commands	Command	Description
	copy running-config startup-config	Saves this configuration change.
	show callhome	Displays Call Home configuration information.
	show running-config callhome	Displays the running configuration information for Call Home.

Send comments to nexus3k-docfeedback@cisco.com

show startup-config eem

To display information about the startup configuration for the Embedded Event Manager (EEM), use the **show startup-config eem** command.

show startup-config eem

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

Defaults	None
-----------------	------

Command Modes	Any command mode
----------------------	------------------

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


Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to display information about the startup configuration for EEM:
-----------------	--

```
switch# show startup-config eem
!Command: show startup-config eem
!Time: Thu Feb 23 02:05:51 2012
!Startup config saved at: Wed Feb 22 20:55:47 2012

version 5.0(3)U5(1)
switch#
```

Related Commands	Command	Description
	show event manager environment	Displays information about the configured environment variables.
	show event manager event-types	Displays information about the event manager event types.
	show event manager history events	Displays the history of events for all policies.
	show event manager policy-state	Displays information about a system policy.
	show event manager script system	Displays information about the script policies.

 show startup-config eem

Send comments to nexus3k-docfeedback@cisco.com

Command	Description
show running-config eem	Displays information about the running configuration for the Embedded Event Manager (EEM).
show event manager system-policy	Displays information about the predefined system policies.

Send comments to nexus3k-docfeedback@cisco.com

show startup-config exclude-provision

To display the startup configuration that excludes the configuration for offline preprovisioned interfaces, use the **show startup-config exclude-provision** command.

show startup-config exclude-provision

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

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

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

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

Examples	<p>This example shows how to display the startup configuration without the offline preprovisioned interfaces:</p> <pre>switch# show startup-config exclude-provision</pre>
-----------------	--

Related Commands	Command	Description
	provision	Preprovisions a module in a slot.
	show provision	Displays the preprovisioned module information.
	show running-config exclude-provision	Displays the running configuration excluding the preprovisioned features.
	slot	Configures a chassis slot for a predefined module.

Send comments to nexus3k-docfeedback@cisco.com

show startup-config ptp

To display the Precision Time Protocol (PTP) startup configuration, use the **show startup-config ptp** command.

show startup-config ptp [all]

Syntax Description	all (Optional) Displays all the default and configured information.				
Command Default	Displays only the configured information.				
Command Modes	EXEC mode				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>5.0(3)U2(2)</td><td>This command was introduced.</td></tr> </table>	Release	Modification	5.0(3)U2(2)	This command was introduced.
Release	Modification				
5.0(3)U2(2)	This command was introduced.				

Examples

This example shows how to display the PTP startup configuration:

```
switch# show startup-config ptp

!Command: show startup-config ptp
!Time: Wed Aug 24 08:10:00 2011
!Startup config saved at: Wed Aug 24 08:09:56 2011

version 5.0(3)U2(2)
feature ptp

ptp domain 1
ptp source 192.0.2.1
ptp priority1 10
ptp priority2 20

interface Ethernet1/5
  ptp
  ptp vlan 5
  ptp delay-request minimum interval 2

switch#
```

This example shows how to display the entire PTP startup configuration, including the default values:

```
switch# show startup-config ptp all
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands	Command	Description
	copy running-config startup-config	Copies the running configuration information to the startup configuration file.
	ptp source	Configures the global source IP for PTP packets.

Send comments to nexus3k-docfeedback@cisco.com

show startup-config vtp

To display the VLAN Trunking Protocol (VTP) configuration from the startup configuration file, use the **show startup-config vtp** command.

show startup-config vtp

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

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

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

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

Examples	<p>This example shows how to display the VTP configuration stored in the startup configuration file:</p> <pre>switch# show startup-config vtp</pre>
-----------------	---

Related Commands	Command	Description
	copy running-config startup-config	Copies the running configuration to the startup configuration file.
	feature vtp	Enables VTP on the switch.
	vtp domain	Configures the VTP administrative domain.
	vtp file	Stores the VTP configuration in a file.
	vtp mode	Configures a VTP device mode.

Send comments to nexus3k-docfeedback@cisco.com

show tech-support callhome

To display the technical support output for Call Home, use the **show tech-support callhome** command.

show tech-support callhome

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

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

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

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

Examples	<p>This example shows how to display the troubleshooting information for Call Home:</p> <pre>switch# show tech-support callhome</pre>
-----------------	---

Related Commands	Command	Description
	show callhome	Displays Call Home configuration information.
	show running-config callhome	Displays the running configuration information for Call Home.

Send comments to nexus3k-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 shut** 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

Release	Modification
5.0(3)U2(2)	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)#
```

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

Send comments to nexus3k-docfeedback@cisco.com

site-id (Call Home)

To configure the optional site number for the customer, use the **site-id** command. To remove a site number, use the **no** form of this command.

site-id *site-number*

no site-id

Syntax Description	<i>site-number</i>	Site number. The site number can be up to 255 alphanumeric characters in free format.
--------------------	--------------------	---

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

Command Modes	Callhome configuration mode
---------------	-----------------------------

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

Usage Guidelines	You can configure the customer identification information that Cisco Smart Call Home should use. The service agreement includes the customer identification information, such as the customer ID, contract ID, and site ID.
------------------	---

Examples	This example shows how to configure a site number:
----------	--

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# site-id 10020-1203
switch(config-callhome)#
```

Related Commands	Command	Description
	switch-priority	Configures the switch priority for the switch.
	show callhome	Displays a summary of the Call Home configuration.

Send comments to nexus3k-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
5.0(3)U1(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 3000 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# configure terminal
switch(config)# snmp-server community public use-acl my_acl_for_public
switch(config)#
```

Send comments to nexus3k-docfeedback@cisco.com

Related Commands

Command	Description
show snmp community	Displays the SNMP community strings.

Send comments to nexus3k-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.



Note Beginning with release 7.0(3)I2(1), **snmp-server contact** no longer has a default name and must be configured to enable callhome.

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
5.0(3)U1(1)	This command was introduced.
7.0(3)I2(1)	This command no longer has a default name and must be configured to enable callhome.

Examples

This example shows how to set an SNMP contact:

```
switch# configure terminal
switch(config)# snmp-server contact DialSystemOperatorAtBeeper#1235
switch(config)#
```

This example shows how to remove an SNMP contact:

```
switch# configure terminal
switch(config)# no snmp-server contact DialSystemOperatorAtBeeper#1235
switch(config)#
```

Related Commands

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
5.0(3)U1(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# configure terminal
switch(config)# snmp-server context public1 vrf default
switch(config)#
```

Send comments to nexus3k-docfeedback@cisco.com

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

Send comments to nexus3k-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] | storm-control [trap-rate val] | vsan | 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] | storm-control [trap-rate] | vsan | zone
[default-zone-behavior-change | merge-failure | merge-success | request-reject1 |
unsupp-mem]]
```

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.
fcdomain	(Optional) Enables notifications for the Fibre Channel domain.
fcns	(Optional) Enables notifications for the name server.
fcs	(Optional) Enables notifications for the fabric configuration server.

Send comments to nexus3k-docfeedback@cisco.com

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.
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.
storm-control	(Optional) Enables the Storm Control trap.
storm-control trap-rate val	(Optional) Specifies the number of Storm Control traps per minute.
vsan	(Optional) Enables notifications for VSANs.
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.

Command Default

All notifications

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)U3(1)	The storm-control option was added.
5.0(3)U1(1)	This command was introduced.

Send comments to nexus3k-docfeedback@cisco.com

Usage Guidelines

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

The **no snmp-server enable traps storm-control** command disables SNMP traps for Storm Control.

Examples

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

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

This example shows how to enable SNMP notifications for Storm Control:

```
switch# configure terminal
switch(config)# snmp-server enable traps storm-control
switch(config)#
```

This example shows how to specify the number of Storm Control traps per minute:

```
switch# configure terminal
switch(config)# snmp-server enable traps storm-control trap-rate 100
switch(config)#
```

This example shows how to disable all SNMP notifications:

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

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 nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
5.0(3)U1(1)	This command was introduced.

Send comments to nexus3k-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# configure terminal
switch(config)# snmp-server enable traps link
switch(config)#
```

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

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

Related Commands

Command	Description
<code>show snmp trap</code>	Displays the SNMP notifications enabled or disabled.

Send comments to nexus3k-docfeedback@cisco.com

snmp-server enable traps vtp

To enable the Simple Network Management Protocol (SNMP) notifications for a VLAN Trunking Protocol (VTP) domain, use the **snmp-server enable traps vtp** command. To disable SNMP notifications on a VTP domain, use the **no** form of this command.

snmp-server enable traps vtp

no snmp-server enable traps vtp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

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

This command does not require a license.

Examples

This example shows how to enable SNMP notifications on a VTP domain:

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

This example shows how to disable all SNMP notifications on a VTP domain:

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

Related Commands

Command	Description
show snmp trap	Displays the SNMP notifications enabled or disabled.
show vtp status	Displays VTP information.

Send comments to nexus3k-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
5.0(3)U1(1)	This command was introduced.

Examples

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

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

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

```
switch# configure terminal
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 nexus3k-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>	Name or Internet address of the 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.

Command Default

Disabled

Send comments to nexus3k-docfeedback@cisco.com

Command Modes Global configuration mode

Command History	Release	Modification
	5.0(3)U1(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# configure terminal
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# configure terminal
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 nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples

This example shows how to set a system location string:

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

This example shows how to remove the system location string:

```
switch# configure terminal
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 nexus3k-docfeedback@cisco.com](mailto:nexus3k-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
5.0(3)U1(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# configure terminal
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# configure terminal
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.

Send comments to nexus3k-docfeedback@cisco.com

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

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

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

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

Related Commands	Command	Description
	show snmp	Displays the SNMP status.

Send comments to nexus3k-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) 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
5.0(3)U1(1)	This command was introduced.

Examples

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

```
switch# configure terminal
```

Send comments to nexus3k-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# configure terminal
switch(config)# no snmp-server user authuser
switch(config)#
```

Related Commands

Command	Description
show snmp user	Displays information about one or more SNMP users.

Send comments to nexus3k-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
----------------------	------------------------------

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

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.
-------------	--

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

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

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

```
switch# configure terminal
```

Send comments to nexus3k-docfeedback@cisco.com

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

Related Commands

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

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-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} [{both | rx | tx}] | vlan
      vlan-num}
```

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

Syntax Description	
interface	Specifies the interface type to use as the source SPAN port.
ethernet slot/port	Specifies the IEEE 802.3z 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 channel-num	Specifies the EtherChannel interface to use as the source SPAN port. The EtherChannel number is from 1 to 4096.
both	(Optional) Specifies both ingress and egress traffic on the source port. Note Applies to ERSPAN source port.
rx	(Optional) Specifies only ingress traffic on the source port. Note Applies to ERSPAN source port.
tx	(Optional) Specifies only egress traffic on the source port. Note Applies to ERSPAN source port.
vlan vlan-num	Specifies the VLAN interface to use as the source SPAN port. The range is from 1 to 3967 and 4048 to 4093.

Command Default None

Command Modes SPAN session configuration mode
ERSPAN session configuration mode

Command History	Release	Modification
	5.0(3)U2(2)	This command was introduced.

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, or a VLAN port. It cannot be a destination port.

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

Send comments to nexus3k-docfeedback@cisco.com

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 nexus3k-docfeedback@cisco.com

source ip (ERSPAN)

To configure the source IP address for an an Encapsulated Remote Switched Port Analyzer (ERSPAN) destination, use the **source ip** command. To remove the source IP configuration, use the **no** form of this command.

source ip *ip_address*

no source ip *ip_address*

Syntax Description	<i>ip_address</i> IP address for the ERSPAN session.									
Command Default	None									
Command Modes	ERSPAN destination configuration mode									
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>5.0(3)U2(2)</td><td>This command was introduced.</td></tr></table>		Release	Modification	5.0(3)U2(2)	This command was introduced.				
Release	Modification									
5.0(3)U2(2)	This command was introduced.									
Usage Guidelines	An ERSPAN destination session supports only one source IP address.									
Examples	<p>This example shows how to configure a source IP address for an ERSPAN session:</p> <pre>switch# configure terminal switch(config)# monitor session 1 type erspan-destination switch(config-erspan-dst)# source ip 192.0.2.1 switch(config-erspan-dst)#</pre>									
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>monitor session</td><td>Creates a new SPAN session configuration.</td></tr><tr><td>show monitor session</td><td>Displays SPAN session configuration information.</td></tr><tr><td>show running-config monitor</td><td>Displays the running configuration information of a SPAN session.</td></tr></table>		Command	Description	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.
Command	Description									
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 nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

streetaddress (Call Home)

To configure the street address for the primary person responsible for the switch, use the **streetaddress** command. To remove the street address, use the **no** form of this command.

streetaddress *address*

no streetaddress

Syntax Description	<i>address</i>	Street address. The address can be a maximum of 255 alphanumeric characters and can include white spaces.
--------------------	----------------	---

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

Command Modes	Callhome configuration mode
---------------	-----------------------------

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

Examples This example shows how to configure the street address for the primary person responsible for the switch:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# streetaddress 170 West Tasman Drive, San Jose, CA 95134-1706
switch(config-callhome)#
```

Related Commands	Command	Description
	contract-id	Configures the contract number for the switch.
	copy running-config startup-config	Saves this configuration change.
	show callhome	Displays a summary of the Call Home configuration.

Send comments to nexus3k-docfeedback@cisco.com

switching-mode store-forward

To enable store-and-forward switching mode on a Cisco NX-OS device, use the **switching-mode store-forward** command. To reenable cut-through switching on a Cisco NX-OS device, use the **no** form of this command.

switching-mode store-forward

no switching-mode store-forward

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration mode

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

Usage Guidelines Enabling store-and-forward switching mode might impact your port-to-port switching latency.
This command does not require a license.

Examples This example shows how to enable store-and-forward switching mode on a Cisco NX-OS device:

```
switch# configure terminal
switch(config)# switching-mode store-forward
switch(config)#
```

This example shows how to reenable cut-through switching mode on a Cisco NX-OS device:

```
switch(config)# no switching-mode store-forward
switch(config)#
```

[Send comments to nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com)

switchport mode monitor buffer-limit

To configure the SPAN buffer limit on a monitor port, use the **switchport mode monitor buffer-limit** command. To remove the configuration and restore the default, use the **no** form of this command.

switchport mode monitor buffer-limit *limit* [bytes | kbytes | mbytes | packets]

no switchport mode monitor buffer-limit *limit* [bytes | kbytes | mbytes | packets]

Syntax Description	<i>limit</i>	Maximum limit.
	bytes	Specifies that the limit value is in bytes. The range is from 1 to 36000.
	kbytes	Specifies that the limit value is in kbytes. The range is from 1 to 7312.
	mbytes	Specifies that the limit value is in mbytes. The range is from 1 to 7.
	packets	Specifies that the limit value is in packets. The range is from 1 to 36000

Command Default SPAN buffer limit default 200 packets.

Command Modes Interface configuration mode

Command History	Release	Modification
	5.0(3)U5(1)	This command was introduced.

Usage Guidelines

This command can be configured on any physical interface.

When configuring a high SPAN buffer limit, it may affect regular data plane traffic as they both use the same memory pool.

This command does not require a license.

Examples This example shows how to configure the SPAN buffer limit to 100 bytes:

```
switch# configure terminal
switch(config)# interface ethernet 1/15
switch(config-if)# switchport monitor
switch(config-if)# switchport mode monitor buffer-limit 100 bytes
switch(config-if)#
```

Related Commands	Command	Description
	show interface ethernet	Displays information about a specified Ethernet interface.

Send comments to nexus3k-docfeedback@cisco.com

switch-priority (Call Home)

To configure the switch priority for the switch, use the **switch-priority** command. To remove the switch priority, use the **no** form of this command.

switch-priority *priority-value*

no switch-priority

Syntax Description

<i>priority-value</i>	Switch priority value. The range is from 0 to 7, with 0 being the highest priority and 7 the lowest.
-----------------------	--

Command Default

Default priority is 7

Command Modes

Callhome configuration mode

Command History

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

Examples

This example shows how to configure the switch priority:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# switch-priority 5
switch(config-callhome)#
```

Related Commands

Command	Description
show callhome	Displays a summary of the Call Home configuration.

Send comments to nexus3k-docfeedback@cisco.com

tag

To correlate multiple events in the policy, use the **tag** command.

tag *tag* {**and** | **andnot** | **or**} *tag* [**and** | **andnot** | **or** {*tag*}]{**happens** *occurs* **in** *seconds*}

Syntax Description		
tag	<i>tag</i>	Tag name. The tag name can be any alphanumeric string up to 29 characters.
and		(Optional) Specifies to use boolean and logic.
andnot		(Optional) Specifies to use boolean andnot logic.
or		(Optional) Specifies to use boolean or logic.
happens		Specifies the number of occurrences before raising the event.
<i>occurs</i>		Number of times that the event occurs. The range is from 1 to 4294967295.
in		Specifies the number of occurrences that must occur within this time period.
<i>seconds</i>		Time in seconds that the next event occurs. The range is from 0 to 4294967295 seconds.

Defaults	None
----------	------

Command Modes	Applet configuration mode
---------------	---------------------------

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

Usage Guidelines	This command does not require a license.
------------------	--

Examples	This example shows how to correlate multiple events in the policy:
----------	--

```
switch# configuration terminal
switch(config)# event manager applet monitorShutdown
switch(config-applet)# description "Monitors interface shutdown."
switch(config-applet)# event cli match "shutdown"
switch(config-applet)# tag one or two happens 1 in 10000
switch(config-applet)# action 1.0 cli show interface ethernet 3/1
```

Related Commands	Command	Description
	description	Configures a descriptive string for the policy.
	event	Configures the event statement for the policy.
	show event-manager policy state	Displays information about the status of the configured policy.

Send comments to nexus3k-docfeedback@cisco.com

terminal event-manager bypass

To specify the command-line interface (CLI) events that match the Embedded Event Manager (EEM) policies to bypass the EEM events, use the **terminal event-manager bypass** command.

terminal event-manager bypass

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Global configuration mode

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

Usage Guidelines This command does not require a license.

Examples This example shows how to specify the command-line interface (CLI) events that match the Embedded Event Manager (EEM) policies to bypass the EEM events:

```
switch# configure terminal
switch(config)# terminal event-manager bypass
switch(config)#
```

Related Commands	Command	Description
	action event-default	Specifies that the default action for the event is to be performed when an EEM applet is triggered.

Send comments to nexus3k-docfeedback@cisco.com

transport email (Call Home)

To configure the Simple Mail Transport Protocol (SMTP) server address for the Call Home functionality to work, and optionally the from and reply-to e-mail addresses, use the **transport email** command. To remove the SMTP server, use the **no** form of this command.

transport email {**from** *email-addr* | **mail-server** *ip-address* [**port** *port-no*] [**priority** *priority-no*] | **reply-to** *email-addr* | **smtp-server** *ip-address* [**port** *port-no*] [**use-vrf** *vrf-name*] }

no transport email {**from** | **mail-server** *ip-address* [**port** *port-no*] [**priority** *priority-no*] | **reply-to** | **smtp-server** }

Syntax Description		
from	<i>email-addr</i>	Specifies the e-mail from field for Call Home messages.
		E-mail address. The address can be a maximum of 255 alphanumeric characters and cannot include white spaces; for example, <i>personname@companyname.com</i> .
mail-server	<i>ip-address</i>	Configures the SMTP server address for supporting multiple SMTP servers.
		Domain name server (DNS) name, IPv4 address, or IPv6 address of the SMTP server.
port <i>port-no</i>		(Optional) Specifies the SMTP server port. The port number range is from 1 to 65535, and the default port number is 25.
priority <i>priority-no</i>		(Optional) Specifies the SMTP server priority. The server priority value range is from 1 to 100, and the default is 50.
reply-to		Specifies the reply-to email address.
smtp-server		Configures the SMTP server address.
use-vrf <i>vrf-name</i>		(Optional) Specifies the virtual routing and forwarding instance (VRF) instance to use when communicating with this SMTP server. The name is case sensitive and has 255 alphanumeric characters.

Command Default	SMTP port number: 25 SMTP server priority: 50
-----------------	--

Command Modes	Callhome configuration mode
---------------	-----------------------------

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

Examples	<p>This example shows how to configure the SMTP server for the Call Home service:</p> <pre> switch# configure terminal switch(config)# callhome switch(config-callhome)# transport email smtp-server 192.0.2.10 use-vrf Red switch(config-callhome)# </pre>
----------	---

Send comments to nexus3k-docfeedback@cisco.com

This example shows how to configure the e-mail from and reply-to field for Call Home messages:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# transport email smtp-server 192.0.2.10 use-vrf Red
switch(config-callhome)# transport email from person@example.com
switch(config-callhome)# transport email reply-to person@example.com
switch(config-callhome)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves this configuration change.
show callhome	Displays Call Home configuration information.
show callhome transport-email	Displays information about the e-mail configuration for Call Home.
transport email	Configures the SMTP server address for Call Home.

Send comments to nexus3k-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
	5.0(3)U1(1)	This command was introduced.

Examples	This example shows how to verify a session:
	<pre>switch# configure session MySession switch(config-s)# verify Failed to start Verification: Session Database already locked, Verify/Commit in Progress. switch(config-s)#</pre>

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

Send comments to nexus3k-docfeedback@cisco.com

vrf (ERSPAN)

To configure a virtual routing and forwarding (VRF) instance for Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic forwarding in the source, use the **vrf** command. To revert to the default settings, use the **no** form of this command.

```
vrf { vrf_name | default | management }
```

```
no vrf { vrf_name | default | management }
```

Syntax Description

<i>vrf_name</i>	Name of the VRF. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.
default	Specifies the default VRF instance.
management	Specifies the management VRF instance.

Command Default

None

Command Modes

ERSPAN session configuration mode

Command History

Release	Modification
5.0(3)U2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a VRF instance for the ESRSPAN source:

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

Related Commands

Command	Description
monitor-session	Enters the monitor configuration mode for configuring an ERSPAN session for analyzing traffic between ports.
show monitor session	Displays information about the Ethernet Switched Port Analyzer (SPAN) or ERSPAN monitor session.