



## **Cisco Nexus 7000 Series NX-OS System Management Command Reference**

December 2016

**Cisco Systems, Inc.**

[www.cisco.com](http://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](http://www.cisco.com/go/offices).

Text Part Number: OL-25806-03

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](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

*Cisco Nexus 7000 Series NX-OS System Management Command Reference*  
©2008–2014 Cisco Systems, Inc. All rights reserved.



**New and Changed Information** 1xvii

**Preface** 1xxiii

Audience 1xxiii

Organization 1xxiii

Document Conventions 1xxiv

Related Documentation 1xxv

Obtaining Documentation and Submitting a Service Request 1xxvi

**A Commands** SM-1

abort (Call home) SM-2

abort (Session Manager) SM-3

action cli SM-4

action counter SM-5

action event-default SM-7

action exceptionlog SM-8

action forceshut SM-10

action overbudgetshut SM-11

action policy-default SM-12

action reload SM-13

action snmp-trap SM-14

action syslog SM-15

alert-group SM-17

**B Commands** SM-19

blink SM-20

**C Commands** SM-23

callhome SM-24

callhome send SM-26

callhome test SM-27

cdp advertise SM-28

cdp enable SM-29

cdp format device-id **SM-30**

cdp holdtime **SM-31**

cdp timer **SM-32**

cfs distribute **SM-33**

cfs eth **SM-34**

cfs ipv4 **SM-35**

cfs region **SM-37**

check logflash **SM-39**

checkpoint **SM-40**

clear callhome session **SM-42**

clear cdp **SM-43**

clear checkpoint database **SM-44**

clear cores **SM-45**

clear flow exporter **SM-46**

clear flow monitor **SM-47**

clear hardware flow ip **SM-49**

clear logging ip access-list cache **SM-51**

clear logging logfile **SM-52**

clear logging nvram **SM-53**

clear logging onboard **SM-54**

clear logging session **SM-56**

clear ntp session **SM-57**

clear ntp statistics **SM-58**

clear nvram **SM-59**

clear platform flow ip **SM-60**

clear processes log archive **SM-62**

clear rmon **SM-63**

clear session state name **SM-64**

clear snmp counters **SM-65**

clear snmp hostconfig **SM-66**

clear system reset-reason **SM-67**

collect counter **SM-68**

collect flow **SM-70**

collect interface **SM-72**

collect routing **SM-74**

[collect timestamp sys-uptime](#) **SM-77**  
[collect transport tcp flags](#) **SM-79**  
[commit \(Call home\)](#) **SM-81**  
[commit \(Session Manager\)](#) **SM-83**  
[configure session](#) **SM-84**  
[contract-id](#) **SM-85**  
[counter](#) **SM-86**  
[customer-id](#) **SM-89**

## **D Commands** **SM-91**

[description \(EEM\)](#) **SM-92**  
[description \(NetFlow record\)](#) **SM-93**  
[description \(NetFlow monitor\)](#) **SM-94**  
[description \(NetFlow exporter\)](#) **SM-95**  
[description \(NetFlow sampler\)](#) **SM-96**  
[description \(SPAN\)](#) **SM-97**  
[destination](#) **SM-98**  
[destination interface \(SPAN\)](#) **SM-99**  
[destination-profile](#) **SM-101**  
[destination-profile alert-group](#) **SM-103**  
[destination-profile email-addr](#) **SM-105**  
[destination-profile format](#) **SM-107**  
[destination-profile http](#) **SM-108**  
[destination-profile message-level](#) **SM-109**  
[destination-profile message-size](#) **SM-110**  
[destination-profile transport-method](#) **SM-111**  
[diagnostic bootup level](#) **SM-112**  
[diagnostic clear result module](#) **SM-113**  
[diagnostic monitor interval module](#) **SM-114**  
[diagnostic monitor module](#) **SM-116**  
[diagnostic ondemand action-on-failure](#) **SM-118**  
[diagnostic ondemand iteration](#) **SM-119**  
[diagnostic start](#) **SM-120**  
[diagnostic stop](#) **SM-121**  
[diagnostic test simulation](#) **SM-122**  
[diagnostic test simulation clear](#) **SM-124**

distribute **SM-125**

dscp **SM-127**

**E Commands** **SM-129**

erspan-id **SM-130**

ethanalyzer local interface **SM-131**

ethanalyzer local read **SM-133**

event cli **SM-134**

event counter **SM-136**

event fanabsent **SM-138**

event fanbad **SM-139**

event gold **SM-140**

event manager applet **SM-142**

event manager clear counter **SM-143**

event manager clear history events **SM-144**

event manager environment **SM-145**

event manager policy **SM-146**

event manager run **SM-147**

event module-failure **SM-148**

event module status **SM-150**

event oir **SM-152**

event policy-default **SM-154**

event snmp **SM-155**

event storm-control **SM-158**

event syslog **SM-159**

event temperature **SM-161**

event track **SM-162**

exporter **SM-164**

**F Commands** **SM-165**

feature lldp **SM-166**

feature netflow **SM-168**

feature ntp **SM-169**

feature ptp **SM-171**

feature scheduler **SM-173**

filter access-group **SM-174**

filter vlan **SM-176**

filter vlan include-untagged **SM-177**

flow exporter **SM-178**

flow monitor **SM-180**

flow record **SM-183**

flow timeout **SM-185**

## **H Commands** **SM-187**

hw-module logging onboard **SM-188**

## **I Commands** **SM-191**

ip access-list **SM-192**

ip dscp **SM-193**

ip flow monitor **SM-194**

ip ttl **SM-197**

## **L Commands** **SM-199**

lldp holdtime **SM-200**

lldp receive **SM-202**

lldp reinit **SM-204**

lldp timer **SM-206**

lldp tlv-select **SM-208**

lldp transmit **SM-210**

locator-led **SM-212**

logging console **SM-214**

logging event **SM-216**

logging ip access-list cache **SM-217**

logging level **SM-219**

logging logfile **SM-221**

logging message interface type ethernet description **SM-223**

logging module **SM-225**

logging monitor **SM-227**

logging server **SM-229**

logging source-interface **SM-231**

logging timestamp **SM-232**

## **M Commands** **SM-233**

match datalink **SM-234**

match ip **SM-236**

[match ipv4](#) **SM-237**  
[match \(NetFlow\)](#) **SM-238**  
[match transport](#) **SM-240**  
[mode](#) **SM-241**  
[monitor counter](#) **SM-242**  
[monitor erspan origin ip-address](#) **SM-244**  
[monitor session](#) **SM-245**  
[mtu](#) **SM-248**  
[multicast best-effort](#) **SM-250**

**N Commands** **SM-253**

[ntp abort](#) **SM-254**  
[ntp access-group](#) **SM-255**  
[ntp authenticate](#) **SM-257**  
[ntp authentication-key](#) **SM-259**  
[ntp commit](#) **SM-261**  
[ntp distribute](#) **SM-262**  
[ntp enable](#) **SM-263**  
[ntp logging](#) **SM-264**  
[ntp master](#) **SM-266**  
[ntp peer](#) **SM-268**  
[ntp server](#) **SM-270**  
[ntp source](#) **SM-272**  
[ntp source-interface](#) **SM-273**  
[ntp sync-retry](#) **SM-274**  
[ntp trusted-key](#) **SM-275**

**O Commands** **SM-277**

[option exporter-stats timeout](#) **SM-278**  
[option interface-table timeout](#) **SM-279**  
[option sampler-table timeout](#) **SM-280**

**P Commands** **SM-281**

[port-monitor activate](#) **SM-282**  
[port-monitor enable](#) **SM-283**  
[port-monitor name](#) **SM-284**  
[port-type](#) **SM-285**



poweroff module **SM-286**  
 power redundancy-mode **SM-287**  
 ptp announce **SM-289**  
 ptp delay-request minimum interval **SM-291**  
 ptp domain **SM-293**  
 ptp pdelay-req-interval **SM-295**  
 ptp priority1 **SM-297**  
 ptp priority2 **SM-298**  
 ptp source **SM-300**  
 ptp sync interval **SM-302**  
 ptp vlan **SM-304**

### **R Commands** **SM-307**

rate-limit **SM-308**  
 record **SM-310**  
 record netflow **SM-311**  
 record netflow ipv4 **SM-312**  
 record netflow ipv6 **SM-313**  
 record netflow-original **SM-314**  
 remote-span **SM-315**  
 rmon alarm **SM-316**  
 rmon event **SM-318**  
 rmon hcalarm **SM-320**  
 role distribute **SM-322**  
 rollback running-config checkpoint **SM-323**

### **S Commands** **SM-325**

sampler **SM-326**  
 save **SM-328**  
 scheduler **SM-329**  
 shut **SM-332**  
 snmp-server aaa-user cache-timeout **SM-333**  
 snmp-server community **SM-334**  
 snmp-server contact **SM-336**  
 snmp-server context **SM-337**  
 snmp-server enable traps **SM-339**  
 snmp-server globalEnforcePriv **SM-343**

snmp-server host	SM-344
snmp-server host filter-vrf	SM-346
snmp-server host use-vrf	SM-347
snmp-server location	SM-348
snmp-server mib community-map	SM-349
snmp-server protocol enable	SM-351
snmp-server source-interface	SM-352
snmp-server tcp-session	SM-354
snmp-server user	SM-355
snmp-server user enforcePriv	SM-357
snmp-trap	SM-358
source	SM-360
source	SM-361
switchport monitor	SM-363
system cores	SM-365
system hap-reset	SM-367
system heartbeat	SM-368
system no hap-reset	SM-369
system no heartbeat	SM-370
system no standby manual-boot	SM-371
system no watchdog	SM-372
system no watchdog kgdb	SM-373
system pss shrink	SM-374
system standby manual-boot	SM-375
system startup-config init	SM-376
system startup-config unlock	SM-377
system test-preupgrade running-ver	SM-378
system switchover	SM-380
system trace	SM-381
system watchdog	SM-382
system watchdog kgdb	SM-383
<b>Show Commands</b>	SM-385
show callhome	SM-386
show callhome transport	SM-388
show cdp	SM-390

show cdp neighbors	SM-392
show cfs application	SM-393
show cfs lock	SM-395
show cfs merge status	SM-397
show cfs peers	SM-399
show cfs regions	SM-401
show cfs status	SM-403
show checkpoint	SM-405
show configuration session	SM-407
show configuration session global-info	SM-409
show cores	SM-410
show diagnostic bootup level	SM-411
show diagnostic content module	SM-412
show diagnostic description module	SM-414
show diagnostic events	SM-415
show diagnostic ondemand setting	SM-417
show diagnostic result	SM-418
show diagnostic simulation	SM-420
show diagnostic status	SM-421
show diff rollback-patch	SM-422
show environment	SM-423
show environment power	SM-426
show event manager environment	SM-428
show event manager event-types	SM-429
show event manager history events	SM-430
show event manager policy	SM-431
show event manager policy-state	SM-432
show event manager script	SM-433
show event manager system-policy	SM-434
show flow exporter	SM-436
show flow interface	SM-438
show flow monitor	SM-440
show flow record	SM-446
show flow timeout	SM-448
show hardware feature-capability	SM-449

show hardware capacity **SM-450**

show hardware capacity interface **SM-452**

show hardware capacity fabric-utilization **SM-454**

show hardware flow aging **SM-456**

show hardware flow entry **SM-458**

show hardware flow ip **SM-460**

show hardware flow sampler **SM-462**

show hardware flow utilization **SM-464**

show inventory **SM-466**

show lldp dcba interface ethernet **SM-468**

show lldp interface ethernet **SM-470**

show lldp neighbors **SM-471**

show lldp timers **SM-473**

show lldp tlv-select **SM-474**

show lldp traffic **SM-475**

show lldp traffic interface ethernet **SM-476**

show locator-led status **SM-478**

show logging console **SM-479**

show logging info **SM-480**

show logging ip access-list cache **SM-482**

show logging last **SM-483**

show logging level **SM-484**

show logging logfile **SM-485**

show logging loopback **SM-486**

show logging module **SM-487**

show logging monitor **SM-488**

show logging nvram **SM-489**

show logging onboard **SM-490**

show logging onboard **SM-497**

show logging server **SM-499**

show logging session status **SM-500**

show logging status **SM-501**

show logging timestamp **SM-502**

show module **SM-503**

show monitor **SM-506**

show monitor session	SM-507
show ntp access-groups	SM-509
show ntp authentication-keys	SM-510
show ntp authentication-status	SM-511
show ntp internal	SM-512
show ntp logging-status	SM-514
show ntp peers	SM-515
show ntp peer-status	SM-516
show ntp pending-diff	SM-517
show ntp pending peers	SM-518
show ntp session status	SM-519
show ntp status	SM-520
show ntp rts-update	SM-521
show ntp source	SM-522
show ntp source-interface	SM-523
show ntp statistics	SM-524
show ntp status	SM-525
show ntp trusted-keys	SM-527
show platform hardware capacity interface resources	SM-528
show port-monitor	SM-529
show port-monitor active	SM-531
show port-monitor status	SM-533
show processes	SM-534
show processes cpu	SM-536
show processes cpu history	SM-537
show process cpu sort	SM-539
show processes log	SM-541
show processes memory	SM-544
show ptp brief	SM-546
show ptp clock	SM-548
show ptp clocks foreign-masters-record	SM-550
show ptp corrections	SM-552
show ptp parent	SM-554
show ptp port	SM-556
show ptp time-property	SM-558

show redundancy status	SM-560
show rmon	SM-562
show running-config cdp	SM-564
show running-config diagnostic	SM-566
show running-config eem	SM-567
show running-config lldp	SM-568
show running-config monitor	SM-569
show running-config netflow	SM-570
show running-config ntp	SM-572
show running-config snmp	SM-574
show sampler	SM-575
show scheduler	SM-576
show snmp	SM-578
show snmp community	SM-581
show snmp context	SM-583
show snmp engineID	SM-584
show snmp group	SM-585
show snmp host	SM-587
show snmp sessions	SM-589
show snmp source-interface	SM-590
show snmp trap	SM-591
show snmp user	SM-593
show sprom	SM-595
show startup-config cdp	SM-598
show startup-config diagnostic	SM-600
show startup-config cfs	SM-601
show startup-config eem	SM-602
show startup-config monitor	SM-603
show startup-config netflow	SM-604
show startup-config ntp	SM-606
show startup-config snmp	SM-608
show system cores	SM-610
show system error-id	SM-611
show system memory-status	SM-612
show system pss shrink status	SM-613

show system pss shrink status details **SM-614**  
show system reset-reason **SM-616**  
show system redundancy **SM-618**  
show system resources **SM-620**  
show system standby manual-boot **SM-621**  
show system uptime **SM-622**  
show tech-support ascii-cfg **SM-623**  
show tech-support cfs **SM-625**  
show tech-support session-mgr **SM-627**  
show tech-support snmp **SM-628**  
show xml server status **SM-629**

### **T Commands** **SM-631**

tag **SM-632**  
template data timeout **SM-634**  
terminal event-manager bypass **SM-635**  
test watchdog **SM-636**  
transport email mail-server **SM-637**  
transport http proxy enable **SM-639**  
transport http proxy server **SM-640**  
transport http use-vrf **SM-641**  
transport udp **SM-642**

### **V Commands** **SM-643**

verify **SM-644**  
version 5 **SM-645**  
version 9 **SM-646**  
vrf **SM-648**

### **X Commands** **SM-651**

xml server max-session **SM-652**  
xml server terminate session **SM-653**  
xml server timeout **SM-654**  
xml server validate **SM-655**

### **System Message Logging Facilities** **SM-657**







## New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 7000 Series NX-OS System Management Command Reference*. The latest version of this document is available at the following Cisco website:

<http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-command-reference-list.html>

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

<http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html>

**Table 1** summarizes the new and changed features for the *Cisco Nexus 7000 Series NX-OS System Management Command Reference*, and tells you where they are documented.

**Table 1**      **New and Changed Features**

Feature	Description	Changed in Release
Fan tray maintenance mode	Modified the <b>hardware fan-tray maintenance-mode</b> command. By default, the fans will now run at 85% speed for approximately 4 minutes when this command is used.	8.1(1)
GIR	Added the <b>system mode maintenance non-interactive</b> , <b>system mode maintenance snapshot-delay</b> and <b>show maintenance snapshot-delay</b> commands.	8.0(1)
Fan tray maintenance mode	Added the <b>hardware fan-tray maintenance-mode</b> command.	7.2(0)D1(1)
Flexible NetFlow	Added the <b>show flow monitor</b> command to replace the deprecated <b>show flow sw-monitor</b> command.	6.2(10)
diagnostic eem action conservative	This command was introduced.	6.2(8)
snmp-server enable traps	The <b>cbgp2</b> keyword was added.	6.2(8)

Table 1 New and Changed Features

Feature	Description	Changed in Release
IP access list logging	This command was introduced.	6.2(6)
	Added parameters to the output of the <b>show logging ip access-list cache</b> command.	
BloggerD	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
Converting CLI Commands to Network Configuration Format	This command was introduced.	6.2(2)
NTP	Added the <b>match-all</b> keyword to the <b>ntp access-group</b> command.	6.2(2)
	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
SPAN	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
	This command was introduced.	6.2(2)
	Added support for F2e Series modules with 100 microseconds and 100 nanoseconds granularity.	6.2(2)
	Added the <b>rx</b> , <b>tx</b> , and <b>shut</b> keywords to the <b>monitor session</b> command.	6.2(2)
This command was introduced.	6.2(2)	
This command was introduced.	6.2(2)	
This command was introduced.	6.2(2)	
System Cores	This command was introduced.	6.2(2)
	Added the <b>5sec</b> , <b>1min</b> , and <b>5min</b> keywords to the <b>show cpu processes sort</b> command.	6.2(2)
	Added the <b>sort</b> keyword to the <b>show processes memory</b> command.	6.2(2)
Troubleshooting Features	This command was introduced.	6.2(2)

**Table 1**      **New and Changed Features**

<b>Feature</b>	<b>Description</b>	<b>Changed in Release</b>
flow timeout	Added the <i>seconds</i> argument for the syntax description and also the note.	6.1(2)
Energy Efficient Ethernet	This command was introduced.	6.1(2)
	This command was introduced.	6.1(2)
	This command was introduced.	6.1(2)
	This command was introduced.	6.1(2)
header-type	This command was introduced.	6.1(1)
monitor erspan granularity	This command was introduced.	6.1(1)
mtu	Starting with 6.1, MTU truncation also support ERSPAN session.	6.1(1)
sampling	This command was introduced.	6.1(1)
show flow timeout	Changed the command output.	6.1(1)
ptp source	<b>vrf</b> option is deprecated in Cisco NX-OS 6.1(1) release.	6.1(1)
show monitor session	Changed the command output for erspan-source sessions.	6.1(1)
NetFlow hardware	The <b>show hardware ip</b> command has been changed to the <b>show hardware flow</b> command.	6.0(1)
Flexible Netflow	The <b>show flow monitor</b> command has been changed to the <b>show flow-sw monitor</b> command.	6.0(1)
Callhome	Added the ability to send HTTP messages through an HTTP proxy server.	5.2(1)
EEM event correlation	Added support for multiple event triggers in a single EEM policy.	5.2(1)
Logging	Added the ability to support descriptions for physical Ethernet interfaces and subinterfaces in the system message log.	5.2(1)
Network Time Protocol	Changed the <b>[no] ntp enable</b> command to the <b>[no] feature ntp</b> command.  Added the ability to configure the device as the NTP authoritative server, enabling it to distribute time even if it is not synchronized to an existing time server.	5.2(1)
Precision Time Protocol	Added support for PTP is a time synchronization protocol nodes distributed across a network. This protocol provides greater accuracy than other time synchronization protocols.	5.2(1)

**Table 1**      **New and Changed Features**

<b>Feature</b>	<b>Description</b>	<b>Changed in Release</b>
SPAN Monitor	Added the ability to configure MTU truncation, the source rate limit, and the multicast best effort mode for each SPAN session and the ability to configure MTU truncation and the multicast best effort mode for each ERSPAN session.	5.2(1)
Encapsulated Remote Switched Port Analyzer (ERSPAN)	You can now configure and monitor ERSPAN for analyzing traffic between ports.	5.1(1)
AAA MSCHAP V2 authentication	Added the <b>mschapv2</b> keyword to the <b>aaa authentication login default</b> and <b>show authentication</b> commands.	4.2(1)
AAA accounting log	Added the <b>last-index</b> and <b>start-seqnum</b> keywords to the <b>show accounting log</b> command.	4.2(1)
802.1x authentication	Added the <b>dot1x pae authenticator</b> command.	4.2(1)
RADIUS statistics	Added the <b>clear radius-server statistics</b> command.	4.2(1)
TACACS+ statistics	Added the <b>clear tacacs-server statistics</b> command.	4.2(1)
TACACS+ command authorization	Added the following commands to support TACACS+ command authorization: <ul style="list-style-type: none"> <li>• <b>aaa test authorization command-type</b></li> <li>• <b>show aaa authorization</b></li> <li>• <b>tacacs-server authorization command login default</b></li> <li>• <b>tacacs-server authorization config-command login default</b></li> <li>• <b>terminal verify-only</b></li> </ul>	4.2(1)
Port Security	Changed the following commands to support support port security on port-channel interfaces: <ul style="list-style-type: none"> <li>• <b>clear port-security</b></li> <li>• <b>switchport port-security</b></li> <li>• <b>switchport port-security aging time</b></li> <li>• <b>switchport port-security aging type</b></li> <li>• <b>switchport port-security mac-address</b></li> <li>• <b>switchport port-security mac-address sticky</b></li> <li>• <b>switchport port-security maximum</b></li> <li>• <b>switchport port-security violation</b></li> </ul>	4.2(1)

**Table 1**      **New and Changed Features**

<b>Feature</b>	<b>Description</b>	<b>Changed in Release</b>
IP ACLs	Added the <b>fragments</b> command to support optimization of fragment handling during IP ACL processing.	4.2(1)
MAC ACLs	Added or changed the following commands to support MAC packet classification: <ul style="list-style-type: none"> <li>• <b>ip port access-group</b></li> <li>• <b>ipv6 port traffic-filter</b></li> <li>• <b>mac packet-classify</b></li> </ul>	4.2(1)
Cisco Fabric Services	Cisco Fabric Services (CFS) distributes data, including configuration changes, to all Cisco NX-OS devices in a network.	4.1(2)
Ethernet Switched Port Analyzer	Cisco Ethernet Switched Port Analyzer (SPAN) destinations are enhanced to support intrusion detection by allowing the following: <ul style="list-style-type: none"> <li>• Injecting packets to disrupt a TCP packet stream.</li> <li>• Enabling a forwarding engine to learn the MAC address of the IDS.</li> </ul>	4.1(2)
Call Home	Call Home is enhanced to support the distribution of configurations using CFS.	4.1(2)
Locator LEDs	Locator LEDs can be configured to blink to help locate them on the system.	4.1(2)
Online diagnostics (GOLD)	Cisco online diagnostics are enhanced to provide viewing of events, and to display diagnostic information in the output of the show module command.	4.1(2)
Syslog	Syslog facilities are updated to include: AMT, CFS, DCBX, LISP, Routing IPv6 Multicast, and Routing Multicast.	4.1(2)
NTP	Added the <b>ntp enable</b> command.	4.0(3)
New <b>show hardware fabric-utilization</b> commands	Adds commands to view hardware fabric utilization.	4.0(3)
SNMP	Added the <b>snmp-server aaa-user cache-timeout</b> and <b>snmp-server protocol</b> commands.	4.0(3)
SNMP—Multiple Instance Support	Adds commands for SNMP context to logical network entity mapping, including protocol instances and virtual routing and forwarding (VRF) instances.	4.0(2)
New NetFlow <b>show</b> commands	Adds commands to view NetFlow hardware flows.	4.0(2)





# Preface

---

This preface describes the audience, organization, and conventions of the *Cisco Nexus 7000 Series NX-OS System Management Command Reference* and how to obtain related documentation.

This chapter includes the following sections:

- [Audience, page 1](#)
- [Organization, page 1](#)
- [Document Conventions, page 2](#)
- [Related Documentation, page 3](#)
- [Documentation Feedback, page 5](#)
- [Obtaining Documentation and Submitting a Service Request, page 5](#)

## Audience

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

## Organization

This reference is organized as follows:

Chapter and Title	Description
<a href="#">A Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter A.
<a href="#">B Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter B.
<a href="#">C Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter C.
<a href="#">D Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter D.
<a href="#">E Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter E.

Chapter and Title	Description
<a href="#">F Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter F.
<a href="#">H Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter H.
<a href="#">I Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter I.
<a href="#">L Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter L.
<a href="#">N Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter N.
<a href="#">M Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter M.
<a href="#">O Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter O.
<a href="#">P Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter P.
<a href="#">R Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter R.
<a href="#">S Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter S, except for <b>show</b> commands.
<a href="#">Show Commands</a>	Describes the Cisco NX-OS system management <b>show</b> commands.
<a href="#">T Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter T.
<a href="#">V Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter V.
<a href="#">X Commands</a>	Describes the Cisco NX-OS system management commands that begin with the letter X.
<a href="#">System Message Logging Facilities</a>	Lists the Cisco NX-OS system message logging facilities.

## Document Conventions

Command descriptions use these conventions:

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

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.



**Tip**

Means *the following information will help you solve a problem*.

## Related Documentation

[Cisco NX-OS](#) includes the following documents:

### Release Notes

*Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x*

### NX-OS Configuration Guides

*Configuring the Cisco Nexus 2000 Series Fabric Extender*

*Cisco Nexus 7000 Series NX-OS Configuration Examples, Release 5.x*

*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*

*Configuring Feature Set for FabricPath*

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

*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*  
*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*  
*Cisco Nexus 7000 Series NX-OS IP SLAs Configuration Guide*  
*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*  
*Cisco Nexus 7000 Series NX-OS LISP Configuration Guide*  
*Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*  
*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide*  
*Cisco Nexus 7000 Series NX-OS OTV Configuration Guide*  
*Cisco Nexus 7000 Series OTV Quick Start Guide*  
*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 6.x*  
*Cisco Nexus 7000 Series NX-OS SAN Switching Configuration Guide*  
*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*  
*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*  
*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x*  
*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*  
*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*  
*Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start*  
*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*

## **NX-OS Command References**

*Cisco Nexus 7000 Series NX-OS Command Reference Master Index*  
*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*  
*Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference*  
*Cisco Nexus 7000 Series NX-OS High Availability Command Reference*  
*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*  
*Cisco Nexus 7000 Series NX-OS IP SLAs Command Reference*  
*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*  
*Cisco Nexus 7000 Series NX-OS LISP Command Reference*  
*Cisco Nexus 7000 Series NX-OS MPLS Command Reference*  
*Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*  
*Cisco Nexus 7000 Series NX-OS OTV Command Reference*  
*Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*  
*Cisco Nexus 7000 Series NX-OS SAN Switching Command Reference*  
*Cisco Nexus 7000 Series NX-OS Security Command Reference*  
*Cisco Nexus 7000 Series NX-OS System Management Command Reference*  
*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference*  
*Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference*  
*Cisco NX-OS FCoE Command Reference for Cisco Nexus 7000 and Cisco MDS 9500*

## Other Software Documents

*Cisco NX-OS Licensing Guide*

*Cisco Nexus 7000 Series NX-OS MIB Quick Reference*

*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 6.x*

*Cisco NX-OS System Messages Reference*

*Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*

*Cisco NX-OS XML Interface User Guide*

## Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com). We appreciate your feedback.

## Communications, Services, and Additional Information

To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).

To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).

To submit a service request, visit [Cisco Support](#).

To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).

To obtain general networking, training, and certification titles, visit [Cisco Press](#).

To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

## Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.





# A Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter A.

# abort (Call home)

To delete a Call home Cisco Fabric Services (CFS) configuration session without applying the configuration, use the **abort** command.

**abort**

---

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

---

**Defaults** None

---

**Command Modes** Call home configuration

---

**SupportedUserRoles** network-admin  
vdc-admin

---

Command History	Release	Modification
	4.1(2)	This command was introduced.

---



---

**Usage Guidelines** The **abort** command is supported only on the device where the CFS fabric lock is acquired. This command does not require a license.

---

**Examples** This example shows how to abort a Call home CFS configuration session:

```
switch(config-callhome)# abort
switch(config-callhome)# show callhome session status
Last Action Time Stamp      : Mon Dec 22 17:34:37 2008
Last Action                  : Abort
Last Action Result           : Success
Last Action Failure Reason   : none
```

---

Related Commands	Command	Description
	<b>show session status</b>	Displays the status of the current CFS configuration session, including the last action and its result.
	<b>callhome</b>	Enters the Call home configuration mode.
	<b>callhome distribute</b>	Enables CFS distribution of the Call home configuration.

---

# abort (Session Manager)

To delete a Session Manager configuration session without applying the configuration, use the **abort** command.

**abort**

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

**Defaults** None

**Command Modes** Session configuration

**SupportedUserRoles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to abort a Session Manager configuration session and show the aborted session:

```
switch(config-s-acl)# abort
switch# show configuration session ACL_permit_tcp
ERROR: Session not found
switch# show configuration session summary
There are no active configuration sessions
```

Related Commands	Command	Description
	<b>show configuration session</b>	Displays the status of the current CFS configuration session, including the last action and its result.
	<b>show configuration session summary</b>	Displays a summary of the configuration session.

# action add

To specify the action of adding values of two variables when an Embedded Event Manager (EEM) applet is triggered, use the **action add** command in applet configuration mode. To undo the add action, use the **no** form of the command.

```
action label add {long-integer | variable-name} {long-integer | variable-name}
```

```
no action label add
```

## Syntax Description

<i>label</i>	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<i>long-integer</i>	Long integer value to be added to a variable.
<i>variable-name</i>	String value to be placed as variable name.

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

The result of **action add** is stored in the variable named `$_result`.

The value of the variable must be a long integer, else the action will fail.

## Examples

This example shows how to add the values of two variables:

```
switch(config)# event manager applet one
switch(config-applet)# action 1.0 set $var1 10
switch(config-applet)# action 1.0 set $var2 20
switch(config-applet)# action 1.0 add $var2 $var1
switch(config-applet)#
```

## Related Commands

Command	Description
<b>event manager applet</b>	Registers the applet with the Embedded Event Manager (EEM)



# action append

To specify the action of appending a string value to a variable value when an Embedded Event Manager (EEM) applet is triggered, use the **action append** command in applet configuration mode. To undo the append action, use the **no** form of the command.

**action** *label* **append** *string* [*variable-value*]

**no action** *label* **append**

## Syntax Description

<i>label</i>	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string</i>	String value to be placed as variable name.
<i>variable-value</i>	(Optional) Long integer value to be appended to the value of string specified.

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

If the variable does not exist, it will be created and set to the given value.

## Examples

The following example shows how to configure an EEM applet to append given string value to the current value of the variable specified:

```
switch(config)# event manager applet one
switch(config-applet)# action 1.0 set $var1 10
switch(config-applet)# action 1.0 append $var1 20
switch(config-applet)#
```

## Related Commands

Command	Description
<b>event manager applet</b>	Registers the applet with the Embedded Event Manager (EEM)

# action break

To specify the action of exiting from a loop of actions when an Embedded Event Manager (EEM) applet is triggered, use the **action break** command in applet configuration mode. To disable the break action, use the **no** form of this command.

**action label break**

**no action label break**

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
--------------	---

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

Use this command to skip all actions down to the related end action.

## Examples

The following example shows how to configure an EEM applet to break from a loop of actions.

```
switch(config)# event manager applet loop
switch(config-applet)# event none
switch(config-applet)# action 1 while 1 eq 1
switch(config-applet)# action 2 break
switch(config-applet)# action 3 end
```

## Related Commands

Command	Description
<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

# action cli

To specify the action of executing a Cisco NX-OS command-line-interface (CLI) command when an Embedded Event Manager (EEM) applet is triggered, use the **action cli** command in applet configuration mode. To remove the action of executing a CLI command, use the **no** form of this command.

```
action label cli { command | local command } cli-string [pattern pattern-string]
```

```
no action label cli
```

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<b>command</b>	Specifies the message to be sent to the Cisco NXOS CLI.
<b>local</b>	Specifies that the action has to be executed on the same card on which the event occurs.
<i>cli-string</i>	CLI command to be executed. If the string contains embedded blanks, enclose it in double quotation marks.
<b>pattern</b> <i>pattern-string</i>	(Optional) Specifies the regular expression response pattern for the <b>command</b> <i>cli-string</i> only when the command string solicits input.

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

The result of the execution of this command is stored in the built-in variable `$_cli_result` that is set when this command is run.

The **action cli** command ends when the solicited prompt as specified in the optional **pattern** keyword is received. Specifying an incorrect pattern will cause the **action cli** command to wait forever until the applet execution times out due to the expiration of the timer.

## Examples

This example shows how to specify an EEM applet to run when the **pattern** keyword specifies the *confirm* argument for the **clear counters Ethernet 0/1** command

```
switch# configure terminal
switch(config)# event manager applet cli-applet
switch(config-applet)# action 1.0 cli command enable
switch(config-applet)# action 1.2 cli command clear counters Ethernet 0/1 pattern confirm
switch(config-applet)# action 3.0 cli command y
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

# action comment

To specify the action of adding comments to an applet when an Embedded Event Manager (EEM) applet is triggered, use the **action comment** command in applet configuration mode. To disable the comment, use the **no** form of this command.

**action** *label* **comment** *string*

**no action** *label* **comment**

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string</i>	Series of characters, including embedded spaces to be placed as comment.

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

Use this command to add comments to applets. This results in a no-operation when the applet is run.

## Examples

The following example shows how to add comments to an applet.

```
switch(config)# event manager applet one
switch(config-applet)# action 1.0 cli comment keyvalue
switch(config-applet)#
```

## Related Commands

Command	Description
<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

# action continue

To specify the action of continuing with a loop of actions when an Embedded Event Manager (EEM) applet is triggered, use the **action continue** command in applet configuration mode. To stop the continue action, use the **no** form of this command.

**action label continue**

**no action label continue**

<b>Syntax Description</b>	<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
---------------------------	--------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Applet configuration (config-applet)
----------------------	--------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.2(0)D1(1)	This command was introduced.

**Examples** The following example shows how to configure an EEM applet to continue with a loop of actions:

```
switch(config)# event manager applet loop
switch(config-applet)# event none
switch(config-applet)# action 1 while 1 eq 1
switch(config-applet)# action 2 continue
switch(config-applet)# action 2 end
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

# action counter

To specify the action of setting or modifying a named counter when an Embedded Event Manager (EEM) applet is triggered, use the **action counter** command in the applet configuration mode. To restore the default value to the counter, use the **no** form of this command.

**action** *label* **counter** **name** *name* **value** *value* **op** {**dec** | **inc** | **nop** | **set**}

**no action** *label* **counter**

## Syntax Description

<b>label</b>	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. If the string contains embedded blanks, enclose it in double quotation marks.
<b>name</b> <i>name</i>	Specifies the name of the counter to be set or modified.  This can be any string value. The counter name is referenced in a registered counter type policy.
<b>value</b> <i>value</i>	Specifies the value to be used to set or modify the counter.  Integer value in the range from -2147483648 to 2147483647 inclusive.
<b>op</b>	Specifies the operation to be performed upon the counter.
<b>dec</b>	Decrements the counter by the specified <i>value</i> .
<b>inc</b>	Increments the counter by the specified <i>value</i> .
<b>nop</b>	Specifies that the counter value is read from the environment variable <code>\$_counter_value_remain</code> .
<b>set</b>	Sets the counter to the value specified in <i>value</i> argument.

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

Use the **event counter** command with the **action counter** command when an event occurs periodically and you want an action to be implemented after a specified number of occurrences of that event.

The environment variable `$_counter_value_remain` is updated when the **action counter** command is completed.

---

**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 set
switch(config-applet)#
```



# action decrement

To specify the action of decrementing the value of a variable when an Embedded Event Manager (EEM) applet is triggered, use the **action decrement** command in applet configuration mode. To remove the action from the applet, use the **no** form of the command.

**action** *label* **decrement** *variable-name* [*long-integer*]

**no action** *label* **decrement**

## Syntax Description

<i>label</i>	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<i>variable-name</i>	String value to be placed as variable name.
<i>long-integer</i>	(Optional) Long integer value by which the variable gets decremented. If it is not specified, a default value of 1 is assumed.

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

None.

## Examples

```
switch(config)# event manager applet one
switch(config-applet)# action 1.0 set varname 10
switch(config-applet)# action 1.0 decrement varname 3
switch(config-applet)#
```

## Related Commands

Command	Description
<b>event manager applet</b>	Registers the applet with the Embedded Event Manager (EEM)

# action divide

To divide the dividend value by the given divisor value when an Embedded Event Manager (EEM) applet is triggered, use the **action divide** command in applet configuration mode. To remove the action from the applet, use the **no** form of the command.

```
action label divide {long-integer1 | variable-name1} {long-integer2 | variable-name2}
```

```
no action label divide
```

## Syntax Description

<i>label</i>	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<i>long-integer1</i>	Dividend integer value for the division.
<i>variable-name1</i>	Value stored in this variable is the dividend for the division. It must be a long integer value.
<i>long-integer2</i>	Divisor integer value for the division.
<i>variable-name2</i>	Value stored in this variable is the divisor for the division. It must be a long integer value.

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## SupportedUserRoles

network-admin

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

All results of the divide action except the remainder are stored in `$_result`.  
The remainder value of the divided integer is stored in `$_remainder`.

## Examples

```
switch(config)# event manager applet one
switch(config-applet)# action 1.0 set varname 10
switch(config-applet)# action 1.0 divide varname 2
switch(config-applet)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>event manager applet</b>	Registers the applet with the Embedded Event Manager (EEM)

# action else

To identify the beginning of an else conditional action block in an if/else condition action block when an Embedded Event Manager (EEM) applet is triggered, use the **action else** command in applet configuration mode. To remove the else conditional action block, use the **no** form of the command.

**action** *label* **else**

**no action** *label* **else**

## Syntax Description

<i>label</i>	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
--------------	---

## Defaults

If the command is not specified within the applet configuration mode, the respective applet is not registered when you exit the configuration.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

If a statement is not associated with this applet, events are still triggered without any action or result. A warning message stating that no statements are associated with this applet is displayed at the exit of the configuration mode.

## Examples

The following example shows how to identify the beginning of an else action block:

```
switch(config)# event manager applet one
switch(config-applet)# action 2.0 if $x eq 0
switch(config-applet)# action 3.0 else
switch(config-applet)# end
```

## Related Commands

Command	Description
<b>event manager applet</b>	Registers the applet with the Embedded Event Manager (EEM)
<b>action elseif</b>	Identifies the beginning of the <b>elseif</b> conditional action block when an EEM applet is triggered.
<b>action if</b>	Identifies the beginning of an <b>if</b> conditional action block when an EEM applet is triggered.



# action elseif

To identify the beginning of an elseif conditional action block in an else / if conditional action block when an Embedded Event Manager (EEM) applet is triggered, use the **action elseif** command in applet configuration mode. To remove the else conditional action block, use the **no** form of the command.

```
action label elseif string-op-1 {eq | gt | ge | lt | le | ne} string-op-2
```

```
no action label elseif
```

## Syntax Description

<i>label</i>	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string-op-1</i>	Sequence of characters that will replace the range of characters in the string.
<b>eq</b>	Compares if two strings are equal.
<b>gt</b>	Checks if <i>string-op-1</i> is greater than <i>string-op-2</i> .
<b>ge</b>	Checks if <i>string-op-1</i> is greater than or equal to <i>string-op-2</i> .
<b>lt</b>	Checks if <i>string-op-1</i> is less than <i>string-op-2</i> .
<b>le</b>	Checks if <i>string-op-1</i> is less than or equal to <i>string-op-2</i> .
<b>ne</b>	Compares if two strings are not equal.
<i>string-op-2</i>	Sequence of characters.

## Defaults

If the command is not specified within the applet configuration mode, the respective applet is not registered when you exit the configuration.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

If a statement is not associated with this applet, events are still triggered without any action or result. A warning message stating that no statements are associated with this applet is displayed at the exit of the configuration mode.

## Examples

The following example shows how to identify the beginning of an elseif conditional action block:

```
switch(config)# event manager applet one
switch(config-applet)# event none
```

```

switch(config-applet)# action 1.0 set x "5"
switch(config-applet)# action 2.0 if $x lt 3
switch(config-applet)# action 3.0 puts $x is less than 3
switch(config-applet)# action 4.0 elseif $x lt 10
switch(config-applet)# action 5.0 puts $x is less than 10
switch(config-applet)# action 6.0 end
switch(config)# event manager run one
5 is less than 10
switch(config)#

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>action else</b>	Identifies the beginning of the <b>else</b> conditional action block when an EEM applet is triggered.
<b>action if</b>	Identifies the beginning of an <b>if</b> conditional action block when an EEM applet is triggered.
<b>action ifgoto</b>	Specifies the applet to jump to the given label if the condition is true when an EEM applet is triggered.

# action end

To identify the end of a conditional action block in the if /else and while conditional action blocks when an Embedded Event Manager (EEM) applet is triggered, use the **action end** command in applet configuration mode. To remove the end conditional action block, use the **no** form of the command.

**action label end**

**no action label end**

## Syntax Description

<i>label</i>	Unique identifier that can be any string value.  Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
--------------	---

## Defaults

If the command is not specified within the applet configuration mode, the respective applet is removed when you exit the configuration.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Examples

The following example shows how to identify the end of a conditional action block

```
switch(config)# event manager applet one
switch(config-applet)# event none
switch(config-applet)# action 1.0 set x '5'
switch(config-applet)# action 2.0 if $x lt 10
switch(config-applet)# action 3.0 puts '$x is less than 10'
switch(config-applet)# action 4.0 end
```

## Related Commands

Command	Description
<b>action else</b>	Identifies the beginning of the <b>else</b> conditional action block when an EEM applet is triggered.
<b>action if</b>	Identifies the beginning of an <b>if</b> conditional action block when an EEM applet is triggered.



# 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* **event-default**

**no action** *label* **event-default**

<b>Syntax Description</b>	<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
---------------------------	--------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Embedded event manager
----------------------	------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(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 1.15 event-default
switch(config-applet)#
```

# action exceptionlog

To log an exception if the specific conditions are encountered when an Embedded Event Manager (EEM) applet is triggered, use the **action exceptionlog** command. To remove the exception log, use the **no** form of this command.

**action** *label* **exceptionlog** **module** *module* **syserr** *error* **devid** *id* **errtype** *type* **errcode** *code*  
**phylayer** *layer* **ports** *list* **harderror** *error* [**desc** *string*]

**no** **action** *label* **exceptionlog** **module** *module* **syserr** *error* **devid** *id* **errtype** *type* **errcode** *code*  
**phylayer** *layer* **ports** *list* **harderror** *error* [**desc** *string*]

## Syntax Description

<b>label</b> <i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<b>module</b> <i>module</i>	Records an exception for the specified module number.
<b>syserr</b> <i>error</i>	Records an exception for the specified system error.
<b>devid</b> <i>id</i>	Records an exception for the specified device ID.
<b>errtype</b> <i>type</i>	Records an exception for the specified error type.
<b>errcode</b> <i>code</i>	Records an exception for the specified error code.
<b>phylayer</b> <i>layer</i>	Records an exception for the specified physical layer.
<b>ports</b> <i>list</i>	Records an exception for the specified ports.
<b>harderror</b> <i>error</i>	Records an exception for the specified hard error.
<b>desc</b> <i>string</i>	(Optional) Specifies a description of the exception logging condition.

## Defaults

None

## Command Modes

Embedded event manager

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

---

**Examples**

This example shows how to log an EEM applet exception:

```
switch# configure terminal
switch(config)# event manager applet exception-applet
switch(config-applet)# action 1.2 exceptionlog module 1 syserr 0x41150010 devid 96 errtype
2 errcode 354 phylayer 0 ports 1-24 harderror false desc "r2d2 general error"
switch(config-applet)#
```

# action exit

To immediately exit from the running applet configuration when an Embedded Event Manager (EEM) applet is triggered, use the **action exit** command in applet configuration mode. To cancel the process of immediate exit from the running applet, use the **no** form of the command.

**action label exit** [*result*]

**no action label exit**

## Syntax Description

<i>label</i>	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<i>result</i>	(Optional) Parameter for the exit result.

## Defaults

If the command is not specified within the applet configuration mode, the respective applet is removed when you exit the configuration.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

If a statement is not associated with the applet, events are still triggered without any action or result. A warning message stating that no statements are associated with this applet is displayed at the exit of the applet configuration mode.

## Examples

The following example shows how to exit the applet configuration mode.

```
switch(config)# event manager applet action
switch(config-applet)# action 4.0 exit 25
```

## Related Commands

Command	Description
<b>event manager applet</b>	Registers the applet with the Embedded Event Manager (EEM)
<b>action else</b>	Identifies the beginning of the <b>else</b> conditional action block when an EEM applet is triggered.
<b>action if</b>	Identifies the beginning of an <b>if</b> conditional action block when an EEM applet is triggered.



# action file

To configure Embedded Event Manager (EEM) applet file operations, use the **action file** command in applet configuration mode. To disable the configuration, use the **no** form of this command.

```
action label file { close file-descriptor | delete file-descriptor | gets file-descriptor variable-name |
open file-descriptor file-name access-permission | puts file-descriptor { string | newline
string } | read file-descriptor variable-name [number] | write file-descriptor string [number] }
```

**no action label file**

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<b>close</b> <i>file-descriptor</i>	Specifies the file to be closed.
<b>delete</b> <i>file-descriptor</i>	Specifies the file to be deleted.
<b>gets</b> <i>file-descriptor</i> <i>variable-name</i>	Specifies the information or the file to be fetched. Specifies variable to store the result of the operation.
<b>open</b> <i>file-descriptor</i> <i>file-name</i>	Specifies the file to be opened. Specifies the name of the file to be opened.
<i>access-permission</i>	Access permission of the file to be opened.
<b>puts</b> <i>file-descriptor</i> <i>string</i>	Specifies the file that will be updated. Data to be put in the file.
<b>newline</b>	Specifies no new line should be added.
<b>read</b> <i>file-descriptor</i>	Specifies the file to read.
<b>write</b> <i>file-descriptor</i>	Specifies the file to write to

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(1)D1(1)	This command was introduced.

## Usage Guidelines

None.

**Examples**

The following example shows how update the file with \$file as file-descriptor.

```
switch(config)# event manager applet action
switch(config-applet)# action 50 file puts $file "keywprd pair"
```

# action forceshut

To configure a forced shutdown of a module, a crossbar ASIC, or the entire switch when an Embedded Event Manager (EEM) applet is triggered, use the **action forceshut** command. To remove the forced shutdown, use the **no** form of this command.

```
action label forceshut [{module module | xbar xbar-number}] reset-reason string
```

```
no action label forceshut [{module module | xbar xbar-number}] reset-reason string
```

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<b>module</b> <i>module</i>	(Optional) Forces a shutdown of the specified module. The module range is from 1 to 10.
<b>xbar</b> <i>xbar-number</i>	(Optional) Forces a shutdown of the specified crossbar ASIC. The ASIC range is from 1 to 5.
<b>reset-reason</b> <i>string</i>	Provides a string that is enclosed in double quotation marks to explain the reason for a forced shutdown.

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure a forced shutdown of module 4 when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet forceshut-applet
switch(config-applet)# action 1.3 forceshut module 4 reset-reason "module 4 failed"
switch(config-applet)#
```



# action foreach

To specify the iteration of an input string using the delimiter as a tokenizing pattern, use the **action foreach** command in applet configuration mode. To remove the iteration of input string, use the **no** form of the command.

**action** *label* **foreach** *string-iterator* *string-input* [*string-delimiter*]

**no action** *label* **foreach**

## Syntax Description

<i>label</i>	Unique identifier that can be any string value.  Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string-iterator</i>	Series of characters that act as an iterator. If the string contains embedded blanks, enclose it in double quotes.
<i>string-input</i>	Series of characters that act as an input. If the string contains embedded blanks, enclose it in double quotes.
<i>string-delimiter</i>	(Optional) Series of characters that act as a delimiter. If the string contains embedded blanks, enclose it in double quotes.  The default delimiter is whitespace.

## Defaults

If the command is not specified within the applet configuration mode, the respective applet is not registered when you exit the configuration.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

The delimiter is a regular expression pattern string. The token found in each iteration is assigned to the given iterator variable.

If a statement is not associated with this applet, events are still triggered without any action or result. A warning message stating that no statements are associated with this applet is displayed at the exit of the configuration.

## Examples

The following example shows how to iterate an input string using the delimiter as a tokenizing pattern:

```
switch(config)# event manager applet action
switch(config-applet)# event none
switch(config-applet)# action 1.0 foreach _iterator ,red blue green orange,
```

■ **action foreach**

```
switch(config-applet)# action 2.0 puts ,iterator is $_iterator,  
switch(config-applet)# action 3.0 end  
switch(config)# event manager run action  
iterator is red iterator is blue iterator is green iterator is orange  
switch(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>event manager applet</b>	Registers the applet with the Embedded Event Manager (EEM)

# action if

To identify the beginning of an if conditional action block when an Embedded Event Manager (EEM) applet is triggered, use the **action if** command in applet configuration mode. To remove the if conditional action block, use the **no** form of the command.

```
action label if string-op-1 {eq | gt | ge | lt | le | ne} string-op-2
```

```
no action label if
```

## Syntax Description

<i>label</i>	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string-op-1</i>	Sequence of characters that will replace the range of characters in the string.
<b>eq</b>	Compares if two strings are equal.
<b>gt</b>	Checks if <i>string-op-1</i> is greater than <i>string-op-2</i> .
<b>ge</b>	Checks if <i>string-op-1</i> is greater than or equal to <i>string-op-2</i> .
<b>lt</b>	Checks if <i>string-op-1</i> is less than <i>string-op-2</i> .
<b>le</b>	Checks if <i>string-op-1</i> is less than or equal to <i>string-op-2</i> .
<b>ne</b>	Compares if two strings are not equal.
<i>string-op-2</i>	Sequence of characters.

## Defaults

If the command is not specified within the applet configuration mode, the respective applet is not registered when you exit the configuration.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

If a statement is not associated with this applet, events are still triggered without any action or result. A warning message stating that no statements are associated with this applet is displayed at the exit of the configuration mode.

## Examples

The following example shows how to identify the beginning of an if conditional action block:

```
switch(config)# event manager applet one
switch(config-applet)# event none
switch(config-applet)# action 1.0 set x "5"
switch(config-applet)# action 2.0 if $x lt 10
```

```
switch(config-applet)# action 3.0 puts "$x is less than 10"  
switch(config-applet)# action 4.0 end  
switch(config)# event manager run one  
5 is less than 10  
switch(config)#
```

---

**Related Commands**

Command	Description
<b>action elseif</b>	Identifies the beginning of the <b>else</b> conditional action block when an EEM applet is triggered.
<b>action ifgoto</b>	Specifies the applet to jump to the given label if the condition is true when an EEM applet is triggered.

---

# action ifgoto

To instruct the applet to jump to a given label if the specified condition is true when an Embedded Event Manager (EEM) applet is triggered, use the **action ifgoto** command in applet configuration mode. To cancel the process of applet jump, use the **no** form of the command.

```
action label-1 if string-op-1 {eq | gt | ge | lt | le | ne} string-op-2 goto label-2
```

```
no action label-1 ifgoto
```

## Syntax Description

<i>label-1</i>	Unique identifier that can be any string value.  Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string-op-1</i>	Sequence of characters that will replace the range of characters in the string.
<b>eq</b>	Compares if two strings are equal.
<b>gt</b>	Checks if <i>string-op-1</i> is greater than <i>string-op-2</i> .
<b>ge</b>	Checks if <i>string-op-1</i> is greater than or equal to <i>string-op-2</i> .
<b>lt</b>	Checks if <i>string-op-1</i> is less than <i>string-op-2</i> .
<b>le</b>	Checks if <i>string-op-1</i> is less than or equal to <i>string-op-2</i> .
<b>ne</b>	Compares if two strings are not equal.
<i>string-op-2</i>	Sequence of characters.
<i>label-2</i>	Unique identifier that can be any string value.  Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.

## Defaults

If the command is not specified within the applet configuration mode, the respective applet is not registered when you exit the configuration.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

If the **goto label** option is used, the **action if** command will not identify the beginning of the action block. Goto actions are supported only within the if/goto format.

To simulate a **goto** without **if**, use a test that is always true.

If a statement is not associated with this applet, events are still triggered without any action or result. A warning message stating that no statements are associated with this applet is displayed at the exit of the configuration mode.

### Examples

The following example shows how to instruct the applet to jump to a given label:

```
switch(config)# event manager applet one
switch(config-applet)# event none
switch(config-applet)# action 1.0 set x "5"
switch(config-applet)# action 2.0 if $x lt 10 goto 4.0
switch(config-applet)# action 3.0 puts "skipping this"
switch(config-applet)# action 4.0 puts "jumped to action 4"
switch(config-applet)# action 5.0 end
switch(config)# event manager run one
jumped to action 4
switch(config)#
```

### Related Commands

Command	Description
<b>action elseif</b>	Identifies the beginning of the <b>else</b> conditional action block when an EEM applet is triggered.
<b>action if</b>	Identifies the beginning of the <b>if</b> conditional action block when an EEM applet is triggered.

# action increment

To specify the action of incrementing the value of a variable when an Embedded Event Manager (EEM) applet is triggered, use the **action increment** command in applet configuration mode. To remove the action from the applet, use the **no** form of the command.

```
action label increment variable-name [long-integer]
```

```
no action label increment
```

Syntax Description		
<i>label</i>	Unique identifier that can be any string value.	
	Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.	
<b>increment</b>	Increments the value of the variable with the long integer specified.	
<i>variable-name</i>	String value placed as variable.	
<i>long-integer</i>	(Optional) Integer value by which the variable value has to be incremented. If this value is not provided, its value is assumed to be 1.	

**Defaults** None

**Command Modes** Applet configuration (config-applet)

**SupportedUserRoles** Network-admin

Command History	Release	Modification
	7.2(0)	This command was introduced.

**Usage Guidelines** The value of the variable must be a long integer.

**Examples**

```
switch(config)# event manager applet one
switch(config-applet)# action 1.0 set var 35
switch(config-applet)# action 1.0 increment var 12
```

Related Commands	Command	Description
	<b>event manager applet</b>	Registers the applet with the Embedded Event Manager (EEM)

# action multiply

To specify the action of multiplying the variable value with a given integer value when an Embedded Event Manager (EEM) applet is triggered, use the **action multiply** command in applet configuration mode. To remove the action from the applet, use the **no** form of the command.

```
action label multiply {long-integer1 | variable-name1} {long-integer2 | variable-name2}
```

```
no action label multiply
```

## Syntax Description

<i>label</i>	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<b>multiply</b>	Multiplies the first parameter value by the second parameter value.
<i>long-integer1</i>	First integer value for the multiplication.
<i>variable-name1</i>	First variable for the multiplication. It must be a long integer value.
<i>long-integer2</i>	Second integer value for the multiplication.
<i>variable-name2</i>	Second variable for the multiplication. It must be a long integer value.

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

The result of the **action multiply** command is stored in `$_result`.

## Examples

```
switch(config)# event manager applet one
switch(config-applet)# action 1.0 multiply 35 23
switch(config-applet)#
```

## Related Commands

Command	Description
<b>event manager applet</b>	Registers the applet with the Embedded Event Manager (EEM)



# action overbudgetshut

To configure the shutdown of a module or the entire switch due to an overbudget power condition when an Embedded Event Manager (EEM) applet is triggered, use the **action overbudgetshut** command. To remove the shutdown configuration, use the **no** form of this command.

**action** *label* **overbudgetshut** [**module** *module*]

**no action** *label* **overbudgetshut** [**module** *module*]

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<b>module</b> <i>module</i>	(Optional) Forces a shutdown of the specified module. For 9slot : The range is from 1 to 9. For 10slot : The range is from 1 to 10. For 18slot : The range is from 1 to 18.

## Defaults

None

(The default action is to powerdown just the linecards starting from slot\_1 till the switch recovers from overbudget condition. In other words, skip both the supervisors (active and standby) and skip all spine/xbars, powerdown lcs starting from slot 1 onwards, till the "Available" power recovers from overbudget condition).

## Command Modes

Applet configuration (config-applet)

## SupportedUserRoles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

---

**Examples**

This example shows how to configure a power overbudget shutdown of module 4 when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet overbudget-applet
switch(config-applet)# action 1.4 overbudgetshut module 4
switch(config-applet)#
```

# action policy-default

To enable the default action(s) 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* **policy-default**

**no action** *label* **policy-default**

<b>Syntax Description</b>	<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
---------------------------	--------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Applet configuration (config-applet)
----------------------	--------------------------------------

<b>SupportedUserRoles</b>	Network-admin
---------------------------	---------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	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 1.65 policy-default
switch(config-applet)#
```

# action publish-event

To specify the action of publishing an application-specific event when the event specified for an Embedded Event Manager (EEM) applet is triggered, use the **action publish-event** command in applet configuration mode. To disable this function, use the **no** form of the command.

**action** *label* **publish-event** **sub-system** *sub-system-id* **type** *event-type* **arg1** *argument-data* [**arg2** *argument-data*] [**arg3** *argument-data*] [**arg4** *argument-data*]

**no** **action** *label* **publish-event**

Syntax Description		
<i>label</i>	Unique identifier that can be any string value.	Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<b>sub-system</b> <i>sub-system-id</i>	Specifies the identifier for the subsystem named in the <i>sub-system-id</i> argument that will publish the application event.	<i>sub-system-id</i> is a number in the range of 1 to 4294967295. If the event is to be published by an EEM policy, the <i>sub-system-id</i> reserved for a customer policy is 798.
<b>type</b> <i>event-type</i>	Specifies the value of an event type within the specified event.	Value of <i>event-type</i> is a number in the range of 1 to 4294967295.
<b>arg1</b>	Specifies that argument data is to be passed to the application-specific event when the event is published.	
<i>argument-data</i>	Character text, an environment variable or a combination of the two. Optional when used with <b>arg2 arg3 arg4</b> .	
<b>arg2 arg3 arg4</b>	(Optional) Specifies that argument data is to be passed to the application-specific event when the event is published.	

**Defaults** None.

**Command Modes** Applet configuration (config-applet)

**SupportedUserRoles** network-admin

Command History	Release	Modification
	7.2(0)D1(1)	This command was introduced.

**Usage Guidelines** None.

**Examples**

The following example shows how a policy named EventPublish\_A runs every 20 seconds and publishes an event to a well-known EEM event type numbered 1. A second policy named EventPublish\_B is registered to run when the well-known EEM event type 1 occurs. When policy EventPublish\_B runs, it outputs a message to syslog containing the argument 1 data passed from EventPublish\_A:

```
switch(config)# event manager applet EventPublish_A
switch(config-applet)# event timer watchdog time 20.0
switch(config-applet)# action 1 syslog msg "Applet EventPublish_A"
switch(config-applet)# action 2 publish-event sub-system 798 type 1 arg1 twenty
switch(config-applet)# exit
switch(config)# event manager applet EventPublish_B
switch(config-applet)# event application sub-system 798 type 1
switch(config-applet)# action 1 syslog msg "Applet EventPublish_B arg1
$_application_data1"
switch(config-applet)#
```

**Related Commands**

Command	Description
<b>event manager applet</b>	Registers the applet with the Embedded Event Manager (EEM)

# action puts

To enable the action of printing data directly to the local terminal (tty) when an Embedded Event Manager (EEM) applet is triggered, use the **action puts** command in applet configuration mode. To disable this function, use the **no** form of the command.

**action** *label* **puts** [**newline**] *string*

**no** **action** *label* **puts**

## Syntax Description

<i>label</i>	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<b>newline</b>	(Optional) Suppresses the display of new line characters.
<i>string</i>	Sequence of characters.

## Defaults

Data is not printed to the local tty.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

**action puts** command applies to synchronous events. The output of this command for a synchronous applet is directly displayed to the tty, bypassing the system logger (syslog).

For an asynchronous applet, the output of this command is directed to the logger.

The **newline** keyword suppresses the display of the newline character.

## Examples

The following example shows how to print data directly to the local tty:

```
switch(config)# event manager applet puts
switch(config-applet)# event none
switch(config-applet)# action 1 regexp "(.*) (.*) (.*)" "one two three" _match _sub1
switch(config-applet)# action 2 puts "match is $_match"
switch(config-applet)# action 3 puts "submatch 1 is $_sub1"
switch(config-applet)# end
switch(config)# event manager run puts
match is one two three submatch 1 is one
switch#
```

Related Commands	Command	Description
	event manager applet	Registers the applet with the Embedded Event Manager (EEM)
	action gets	Gets input from the local tty and stores the value in the given variable.

# action reload

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

**action** *label* **reload** [**module** *module-number*]

**no action** *label* **reload**

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<b>module</b> <i>module-number</i>	Specifies a particular module to be reloaded.

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
4.0(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 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)#
```



# action regexp

To match a regular expression pattern with an input string when an Embedded Event Manager (EEM) applet is triggered, use the **action regexp** command in applet configuration mode. To disable the function, use the **no** form of this command.

```
action label regexp string-pattern string-input [string-match [string-submatch1]
[string-submatch2] [string-submatch3]]
```

```
no action label regexp
```

Syntax Description		
<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.	
<b>regexp</b>	Specifies the regular expression pattern that needs to be compared.	
<i>string-pattern</i>	Sequence of characters to be used as regular expression for pattern matching.	
<i>string-input</i>	Sequence of characters used as input string.	
<i>string-match</i>	(Optional) Name of the variable that stores the entire pattern match.	
<i>string-submatch</i>	(Optional) Name of the variable that stores any sub matches that are present. A maximum of three sub match strings can be specified.	

**Defaults** None

**Command Modes** Applet configuration (config-applet)

Command History	Release	Modification
	7.2(0)D1(1)	This command was introduced.

**Usage Guidelines** The argument *string-pattern* is a regular expression. If some part of the *string-input* matches the pattern, it returns 1; otherwise it returns 0. This result is stored in the inbuilt variable `$_regexp_result`.

The optional *string-match* and *string-submatch* arguments store the results of the match.

**Examples** This example shows how to define a regular expression match:

```
switch(config)# event manager applet regexp
switch(config-applet)# event none
switch(config-applet)# action 1.0 regexp "(.*) (.*) (.*)" "one two three" _match _sub1
switch(config-applet)# action 1.2 puts "match is $_match"
switch(config-applet)# action 1.4 puts "submatch 1 is $_sub1"
switch(config-applet)# event manager run regexp
match is one two three submatch 1 is one
switch(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

# action set

To set the value of a variable when an Embedded Event Manager (EEM) applet is triggered, use the **action set** command in applet configuration mode. To disable this function, use the **no** form of the command.

**action** *label set* *variable-name* *variable-value*

**no action** *label set*

## Syntax Description

<i>label</i>	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<i>variable-name</i>	Name assigned to the variable to be set.
<i>variable-value</i>	Value of the variable.

## Defaults

No variable value is set.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

Use the **action set** command to set the value of a variable when an EEM applet is triggered.

## Examples

The following example shows how to set the value of a variable:

```
switch(config)# event manager applet set
switch(config-applet)# event none
switch(config-applet)# action 1 set str "this is some text"
switch(config-applet)# action 2 string range "$str" 0 6
switch(config-applet)# action 3 puts "$_string_result"
switch(config-applet)# end
switch# event manager run set
this is
switch#
```

## Related Commands

Command	Description
<b>event manager applet</b>	Registers the applet with the Embedded Event Manager (EEM)



## 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 snmp-trap [intdata1 integer] [intdata2 integer] [strdata string]
```

```
no action label snmp-trap [intdata1 integer] [intdata2 integer] [strdata string]
```

### Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<b>intdata1</b> <i>integer</i>	(Optional) Specifies an integer to be sent in the SNMP trap message to the SNMP agent.
<b>intdata2</b> <i>integer</i>	(Optional) Specifies a second integer to be sent in the SNMP trap message to the SNMP agent.
<b>strdata</b> <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.

### Defaults

None

### Command Modes

Applet configuration (config-applet)

### Command History

Release	Modification
4.0(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)#
```

# action string compare

To compare two unequal strings when an Embedded Event Manager (EEM) applet is triggered, use the **action string compare** command in applet configuration mode. To disable the function, use the **no** form of this command.

```
action label string compare [nocase] [length integer] string1 string2
```

```
no action label string compare
```

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<b>nocase</b>	(Optional) Specifies case insensitive comparison of strings.
<b>length</b> <i>integer</i>	(Optional) Specifies the length of the value to limit the comparison. Value of <b>length</b> can range from 1 to 2146483647
<i>string1</i>	Sequence of characters to compare. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string2</i>	Sequence of characters to compare. If the string contains embedded blanks, enclose it in double quotation marks

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

String comparisons are performed on a byte-by-byte basis, from left to right. The command **action string compare** forces a comparison between two unequal strings, followed by integer comparison of the result of string comparison.

When two equal strings are compared, the result is 0. When two unequal strings are compared, if the first string is longer, the result is 1 and if the second string is longer than the first, the result is -1.

The result of string comparison is stored in the inbuilt variable `$_string_result`.

## Examples

This example shows how to compare two unequal strings:

```
switch(config)# event manager applet strcompare
switch(config-applet)# event none
switch(config-applet)# action 1.0 set str "this contains some $str"
switch(config-applet)# action 1.2 string compare nocase length 3 "contains" "$str"
```

Related Commands	Command	Description
	<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

# action string equal

To verify if two strings are equal when an Embedded Event Manager (EEM) applet is triggered, use the **action string equal** command in applet configuration mode. To disable the function, use the **no** form of this command.

```
action label string equal [nocase] [length integer] string1 string2
```

```
no action label string equal
```

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<b>nocase</b>	(Optional) Specifies case insensitive comparison of strings.
<b>length</b> <i>integer</i>	(Optional) Specifies the length of the value to limit the comparison. Value of <b>length</b> can range from 1 to 2146483647.
<i>string1</i>	Sequence of characters to compare.If the string contains embedded blanks, enclose it in double quotation marks
<i>string2</i>	Sequence of characters to compare.If the string contains embedded blanks, enclose it in double quotation marks

## Defaults

Strings are not verified as equal.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

If two strings are equal, it returns 1.

The result of string comparison is stored in the inbuilt variable `$_string_result`.

## Examples

This example shows how to verify if two strings are equal:

```
switch(config)# event manager applet strequal
switch(config-applet)# event none
switch(config-applet)# action 1.0 set str "this contains some data"
switch(config-applet)# action 1.2 string equal "contains" "$str"
```



Related Commands	Command	Description
	<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

## action string first

To get the index of the first occurrence of *string1* within *string2* when an Embedded Event Manager (EEM) applet is triggered, use the **action string first** command in applet configuration mode. To disable the function, use the **no** form of this command.

```
action label string first string1 string2 [index-value]
```

```
no action label string first
```

### Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string1</i>	Sequence of characters to compare.If the string contains embedded blanks, enclose it in double quotation mark
<i>string2</i>	Sequence of characters to compare.If the string contains embedded blanks, enclose it in double quotation mark
<i>index-value</i>	(Optional) The index value to begin the first test. Index value is in the range of 0 to 2147483647.

### Defaults

The index is not returned on the first occurrence of *string1* within *string2*.

### Command Modes

Applet configuration (config-applet)

### Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

### Usage Guidelines

On the first occurrence of *string1*, the index is placed in *string2*. If *string1* is not found, it returns -1. The result of string comparison is stored in the inbuilt variable `$_string_result`.

### Examples

This example shows how to get the index of the first occurrence of *string1* within *string2*:

```
switch(config)# event manager applet strfirst
switch(config-applet)# event none
switch(config-applet)# action 1.0 set str "this contains some data"
switch(config-applet)# action 1.2 string first "contains" "$str"
switch(config-applet)# action 1.2 puts "$_string_result"
switch# event manager run strfirst
5
switch#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>action string last</b>	Returns the index of the last occurrence of <i>string1</i> within <i>string2</i>
<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

# action string index

To get the characters specified at a given index value when an Embedded Event Manager (EEM) applet is triggered, use the **action string index** command in applet configuration mode. To disable the function, use the **no** form of this command.

```
action label string index string [value | end]
```

```
no action label string index
```

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string</i>	Sequence of characters to compare. If the string contains embedded blanks, enclose it in double quotation mark
<i>value</i>	(Optional) The index value which is in the range of 0 to 2147483647
<i>end</i>	(Optional) Last character of the string.

## Defaults

The characters specified at a given index value are not returned.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

The index count starts from zero. Use the *end* argument for the last character of the string.

The command stores the characters in the inbuilt variable `$_string_result`.

## Examples

This example shows how to get the character specified at a given index value:

```
switch(config)# event manager applet index
switch(config-applet)# event none
switch(config-applet)# action 1.0 set str "this is text"
switch(config-applet)# action 1.2 string index "$str" 8
switch(config-applet)# action 1.2 puts "$_string_result"
switch# event manager run index
t
switch#
```

Related Commands	Command	Description
	<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

## action string last

To get the index of the last occurrence of *string1* within *string2* when an Embedded Event Manager (EEM) applet is triggered, use the **action string last** command in applet configuration mode. To disable the function, use the **no** form of this command.

```
action label string last string1 string2 [index-value]
```

```
no action label string last
```

### Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string1</i>	Sequence of characters to compare.If the string contains embedded blanks, enclose it in double quotation mark
<i>string2</i>	Sequence of characters to compare.If the string contains embedded blanks, enclose it in double quotation mark
<i>index-value</i>	(Optional) The index value to begin the last test. Index value is in the range of 0 to 2147483647.

### Defaults

The index is not returned on the last occurrence of *string1* within *string2*.

### Command Modes

Applet configuration (config-applet)

### Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

### Usage Guidelines

On the last occurrence of *string1*, the index is placed in *string2*. If *string1* is not found, it returns -1. The result of string comparison is stored in the inbuilt variable `$_string_result`.

### Examples

This example shows how to get the index of the last occurrence of *string1* within *string2*:

```
switch(config)# event manager applet strlast
switch(config-applet)# event none
switch(config-applet)# action 1.0 set str "this contains some data in data file"
switch(config-applet)# action 1.2 string last "data" "$str"
switch(config-applet)# action 1.2 puts "$_string_result"
switch# event manager run strlast
28
switch#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>action string first</b>	Returns the index of the first occurrence of <i>string1</i> within <i>string2</i>
<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

# action string length

To get the number of characters in a string when an Embedded Event Manager (EEM) applet is triggered, use the **action string length** command in applet configuration mode. To disable the function, use the **no** form of this command.

**action** *label* **string length** *string*

**no** **action** *label* **string length**

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string</i>	Sequence of characters to compare. If the string contains embedded blanks, enclose it in double quotation marks.

## Defaults

The number of characters in a string are not returned.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

The result of the command is stored the in the inbuilt variable `$_string_result`.

## Examples

This example shows how to get the number of characters in a string:

```
switch(config)# event manager applet length
switch(config-applet)# event none
switch(config-applet)# action 1.2 string length "contains"
switch(config-applet)# action 2.0 puts "$_string_result"
switch# event manager run length
8
switch#
```

## Related Commands

Command	Description
<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.



# action string match

To match a pattern of characters with a string when an Embedded Event Manager (EEM) applet is triggered, use the **action string match** command in applet configuration mode. To disable the function, use the **no** form of this command.

```
action label string match [nocase] string-pattern string
```

```
no action label string match
```

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<b>nocase</b>	(Optional) Specifies case insensitive comparison.
<i>string-pattern</i>	String pattern for comparison. Use the following symbols to indicate one or more wildcards, if you use a substring: <ul style="list-style-type: none"> <li>• * - to match against more than one wildcard character</li> <li>• ? - to match against a single wildcard character.</li> </ul>
<i>string</i>	Sequence of characters to compare. If the string contains embedded blanks, enclose it in double quotation mark

## Defaults

Results of pattern matching of strings are not returned to the variable `$_string_result`

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

If the string matches the specified pattern, result is 1; if the string does not match the specified pattern, the result is 0.

The result of the command is stored the in the inbuilt variable `$_string_result`.

## Examples

This example shows how to match a string pattern with a string:

```
switch(config)# event manager applet match
```

## ■ action string match

```

switch(config-applet)# event none
switch(config-applet)# action 1.0 set str "NULL BBB"
switch(config-applet)# action 2.0 string match "*NULL*" "$str"
switch(config-applet)# action 3.0 puts "$_string_result"
switch(config-applet)# end
switch# event manager run match
1
switch#

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

# action string range

To store a range of characters in a string when an Embedded Event Manager (EEM) applet is triggered, use the **action string range** command in applet configuration mode. To disable the function, use the **no** form of this command.

**action** *label* **string range** *string start-index end-index*

**no action** *label* **string range**

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string</i>	Sequence of characters. If the string contains embedded blanks, enclose it in double quotation mark.
<i>start-index</i>	Starting index string value. The range is from 0 to 2147483647
<i>end-index</i>	Ending index string value. The range is from 0 to 2147483647.

## Defaults

A string is not stored.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

The *start-index* and *end-index* arguments specify the range of characters in a string on which to operate. The result of the command is stored in the built-in variable `$_string_result`.

## Examples

This example shows how to store a range of characters in a specified string:

```
switch(config)# event manager applet store
switch(config-applet)# event none
switch(config-applet)# action 1.0 set str "This is some text"
switch(config-applet)# action 2.0 string range "$string" 0 6
switch(config-applet)# action 3.0 puts "$_string_result"
switch(config-applet)# end
switch# event manager run store
This is
switch#
```

■ action string range

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

# action string replace

To store a new string by replacing the range of characters in the specified string when an Embedded Event Manager (EEM) applet is triggered, use the **action string replace** command in applet configuration mode. To disable the function, use the **no** form of this command.

**action** *label* **string replace** *string start-index end-index* [*new-string*]

**no action** *label* **string replace**

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string</i>	Sequence of characters. If the string contains embedded blanks, enclose it in double quotation mark.
<i>start-index</i>	Starting index string value. The range is from 0 to 2147483647
<i>end-index</i>	Ending index string value. The range is from 0 to 2147483647.
<i>new-string</i>	(Optional) Sequence of characters that will replace the range of characters in the string.

## Defaults

A string is not stored.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

Use the **action string replace** command to get a new string by replacing specific characters in a particular string when an EEM applet is triggered. If the value for new-string argument is not specified, the characters are replaced with white space.

The result of the command is stored the in the built-in variable `$_string_result`.

## Examples

This example shows how to store a range of characters in a specified string:

```
switch(config)# event manager applet repalce
switch(config-applet)# event none
switch(config-applet)# action 1.0 set str "This is some text"
switch(config-applet)# action 2.0 string replace "$str" 0 6 "that was"
switch(config-applet)# action 3.0 puts "$_string_result"
switch(config-applet)# end
switch# event manager run replace
that was some text
switch#
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

---

# action string tolower

To store a specific range of characters of a string in lowercase when an Embedded Event Manager (EEM) applet is triggered, use the **action string tolower** command in applet configuration mode. To disable the function, use the **no** form of this command.

```
action label string tolower string [start-index] [end-index]
```

```
no action label string tolower
```

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string</i>	Sequence of characters that needs to be changed to lower case. If the string contains embedded blanks, enclose it in double quotation mark.
<i>start-index</i>	(Optional) Starting index string value. The range is from 0 to 2147483647
<i>end-index</i>	(Optional) Ending index string value. The range is from 0 to 2147483647.

## Defaults

A string is not stored.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

Use the **action string tolower** command to store a specific range of characters in lower case when an EEM applet is triggered. The *start-index* and *end-index* arguments specify the range of characters on which to operate.

The result of the command is stored the in the built-in variable `$_string_result`.

## Examples

This example shows how to convert a range of characters in a specified string, to lower case:

```
switch(config)# event manager applet lowercase
switch(config-applet)# event none
switch(config-applet)# action 1.0 set str "This is a STRING"
switch(config-applet)# action 2.0 string tolower "$str" 11 16
switch(config-applet)# action 3.0 puts "$_string_result"
switch(config-applet)# end
switch# event manager run lowercase
string
switch#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>action string toupper</b>	Stores a specific range of characters of a string in upper case.
	<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.



# action string toupper

To store a specific range of characters of a string in uppercase when an Embedded Event Manager (EEM) applet is triggered, use the **action string toupper** command in applet configuration mode. To disable the function, use the **no** form of this command.

```
action label string toupper string [start-index] [end-index]
```

```
no action label string toupper
```

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string</i>	Sequence of characters that needs to be changed to upper case. If the string contains embedded blanks, enclose it in double quotation mark.
<i>start-index</i>	(Optional) Starting index string value. The range is from 0 to 2147483647
<i>end-index</i>	(Optional) Ending index string value. The range is from 0 to 2147483647.

## Defaults

A string is not stored.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

Use the **action string toupper** command to store a specific range of characters in upper case when an EEM applet is triggered. The *start-index* and *end-index* arguments specify the range of characters on which to operate.

The result of the command is stored the in the built-in variable `$_string_result`.

## Examples

This example shows how to convert a range of characters in a specified string, to lower case:

```
switch(config)# event manager applet uppercase
switch(config-applet)# event none
switch(config-applet)# action 1.0 set str "This is a string"
switch(config-applet)# action 2.0 string tolower "$str" 11 16
switch(config-applet)# action 3.0 puts "$_string_result"
switch(config-applet)# end
switch# event manager run uppercase
STRING
switch#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>action string tolower</b>	Stores a specific range of characters of a string in lower case.
<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

# action string trim

To trim a string when an Embedded Event Manager (EEM) applet is triggered, use the **action string trim** command in applet configuration mode. To disable the function, use the **no** form of this command.

```
action label string trim string1 [string2]
```

```
no action label string trim
```

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string1</i>	Sequence of characters on which the trim action is to be performed. If the string contains embedded blanks, enclose it in double quotation mark.
<i>string2</i>	(Optional) Sequence of characters that needs to be trimmed from <i>string1</i> . If the string contains embedded blanks, enclose it in double quotation mark.  Default value is whitespace.

## Defaults

None.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

Use the **action string trim** command to trim the characters in a string when an EEM applet is triggered. The command trims characters in *string2* from both ends of *string1*. By default, *string2* is whitespace. The result of the command is stored in the built-in variable `$_string_result`.

## Examples

This example shows how to trim a string:

```
switch(config)# event manager applet trim
switch(config-applet)# event none
switch(config-applet)# action 1.0 set str "Hello How are you? Hello"
switch(config-applet)# action 2.0 string trim "$str" "Hello"
switch(config-applet)# action 3.0 puts "$_string_result"
switch(config-applet)# end
switch# event manager run trim
How are you?
switch#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>action string trimleft</b>	Trims the characters of one string from the left end of another string.
<b>action string trimright</b>	Trims the characters of one string from the right end of another string.
<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

# action string trimleft

To trim the characters of one string from the left end of another string when an Embedded Event Manager (EEM) applet is triggered, use the **action string trimleft** command in applet configuration mode. To disable the function, use the **no** form of this command.

```
action label string trimleft string1 [string2]
```

```
no action label string trimleft
```

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string1</i>	Sequence of characters on which the trim action is to be performed. If the string contains embedded blanks, enclose it in double quotation mark.
<i>string2</i>	(Optional) Sequence of characters that needs to be trimmed from <i>string1</i> . If the string contains embedded blanks, enclose it in double quotation mark.  Default value is whitespace.

## Defaults

None.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

Use the **action string trimleft** command to trim a string from left end of another string when an EEM applet is triggered. The command trims characters specified by *string2* from the left end of *string1*. By default, *string2* is whitespace.

The result of the command is stored the in the built-in variable `$_string_result`.

## Examples

This example shows how to trim a string:

```
switch(config)# event manager applet trimleft
switch(config-applet)# event none
switch(config-applet)# action 1.0 set str "Hello How are you?"
switch(config-applet)# action 2.0 string trimleft "$str" "Hello"
switch(config-applet)# action 3.0 puts "$_string_result"
switch(config-applet)# end
switch# event manager run trimleft
How are you?
switch#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>action string trim</b>	Trims a string.
<b>action string trimright</b>	Trims the characters of one string from the right end of another string.
<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.

# action string trimright

To trim the characters of one string from the right end of another string when an Embedded Event Manager (EEM) applet is triggered, use the **action string trimright** command in applet configuration mode. To disable the function, use the **no** form of this command.

```
action label string trimright string1 [string2]
```

```
no action label string trimright
```

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string1</i>	Sequence of characters on which the trim action is to be performed. If the string contains embedded blanks, enclose it in double quotation mark.
<i>string2</i>	(Optional) Sequence of characters that needs to be trimmed from <i>string1</i> . If the string contains embedded blanks, enclose it in double quotation mark.  Default value is whitespace.

## Defaults

None.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(1)	This command was introduced.

## Usage Guidelines

Use the **action string trimright** command to trim a string from right end of another string when an EEM applet is triggered. The command trims characters specified by *string2* from right end of *string1*. By default, *string2* is whitespace.

The result of the command is stored the in the built-in variable `$_string_result`.

## Examples

This example shows how to trim a string:

```
switch(config)# event manager applet trimright
switch(config-applet)# event none
switch(config-applet)# action 1.0 set str "How are you? Hello"
switch(config-applet)# action 2.0 string trimright "$str" "Hello"
switch(config-applet)# action 3.0 puts "$_string_result"
switch(config-applet)# end
switch# event manager run trimright
How are you?
switch#
```

Related Commands	Command	Description
	<b>action string trim</b>	Trims a string.
	<b>action string trimleft</b>	Trims the characters of one string from the left end of another string.
	<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM) and enters the applet configuration mode.



# action subtract

To specify the action of subtracting the value of a variable from another value when an Embedded Event Manager (EEM) applet is triggered, use the **action subtract** command in applet configuration mode. To remove the action from the applet, use the **no** form of the command.

```
action label subtract {long-integer1 | variable-name1} {long-integer2 | variable-name2}
```

```
no action label subtract
```

## Syntax Description

<i>label</i>	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<b>subtract</b>	Subtracts the value of a variable from another variable.
<i>long-integer1</i>	First integer value for the subtraction.
<i>variable-name1</i>	First variable for the subtraction. It must be a long integer value.
<i>long-integer2</i>	Second integer value for the subtraction.
<i>variable-name2</i>	Second variable for the subtraction. It must be a long integer value.

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

Use this command to subtract the value of the second parameter from the first parameter. The result of the **action subtract** command is stored in `$_result`.

## Examples

```
switch(config)# event manager applet one
switch(config-applet)# action 1.0 set var 37
switch(config-applet)# action 1.0 subtract var 26
switch(config-applet)#
```

## Related Commands

Command	Description
<b>event manager applet</b>	Registers the applet with the Embedded Event Manager (EEM)

# 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 syslog [priority {prio | prio-str}] msg msg-text
```

```
no action label syslog [priority {prio | prio-str}] msg msg-text
```

## Syntax Description

<i>label</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. If the string contains embedded blanks, enclose it in double quotation marks.
<b>priority</b>	(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>prio</i>	Priority level: <ul style="list-style-type: none"> <li>• <b>emergencies</b>—Specifies the system is unusable.</li> <li>• <b>alerts</b>—Specifies immediate action is needed.</li> <li>• <b>critical</b>—Specifies critical conditions.</li> <li>• <b>errors</b>—Specifies error conditions.</li> <li>• <b>warnings</b>— Specifies warning conditions.</li> <li>• <b>notifications</b>—Specifies normal but significant conditions.</li> <li>• <b>informational</b>—Specifies informational messages. This is the default.</li> <li>• <b>debugging</b>—Specifies debugging messages.</li> </ul>
<i>prio-str</i>	A \$-prefixed parameter that you previously set to a priority level.
<b>msg</b> <i>msg-text</i>	Specifies the message to be logged. The <i>msg-text</i> can contain character text, an environment variable, or a combination of the two. If the string contains embedded blanks, enclose it in double quotation marks.

## Defaults

None

## Command Modes

Embedded event manager

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

Messages written to syslog from an EEM applet are not screened for EEM syslog events, which may 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.

---

**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 "Syslog condition: $log"
switch(config-applet)#
```

# action while

To identify the beginning of a loop of a conditional block when an Embedded Event Manager applet is triggered, use the **action while** command in applet configuration mode. To disable this function, use the **no** form of the command.

**action** *label* **while** *string1* *operator* *string2*

**no** **action** *label* **while**

## Syntax Description

<i>label</i>	Unique identifier that can be any string value. Actions are sorted and run in an ascending alphanumeric key sequence using the <i>label</i> as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
<i>string1</i>	First operand.
<i>operator</i>	Value used with <i>string1</i> and <i>string2</i> operands to determine how the current counter value is compared to the entry value or exit value. Valid values are: <ul style="list-style-type: none"> <li>gt - greater than</li> <li>ge - greater than or equal to</li> <li>eq - equal to</li> <li>ne - not equal to</li> <li>lt - less than</li> <li>le - less than or equal to</li> </ul>
<i>string2</i>	Second operand.

## Defaults

None.

## Command Modes

Applet configuration (config-applet)

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

Use the **action while** command to identify the beginning of a loop conditional block.

If *\$\_variable* is found within a string, it will be substituted before the expression is tested.

## Examples

The following example shows how to identify the beginning of a loop conditional block when an EEM applet is triggered:

```
switch(config)# event manager applet action
switch(config-applet)# action 1.0 set _i 2
switch(config-applet)# action 2.0 while $_i lt 10
switch(config-applet)# action 3.0 action syslog msg ,i is $_i,
switch(config-applet)# action 4.0 end
```

**Related Commands**

Command	Description
<b>event manager applet</b>	Registers the applet with the Embedded Event Manager (EEM)
<b>action else</b>	Identifies the beginning of an else block in the if/else conditional block
<b>action elseif</b>	Identifies the beginning of the if/else conditional block.
<b>action if</b>	Identifies the beginning of an if conditional block.

# alert-group

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

```
alert-group { All | Configuration | Diagnostic | EEM | Environmental | Inventory | License |
Linecard-Hardware | Supervisor-Hardware | Syslog-group-port | System | Test }
user-def-cmd cli_command
```

```
no alert-group { All | Configuration | Diagnostic | Environmental | Inventory | License |
Linecard-Hardware | Supervisor-Hardware | Syslog-group-port | System | Test }
user-def-cmd cli_command
```

## Syntax Description

<b>All</b>	Specifies all alert groups—configuration, diagnostic, EEM, environmental, inventory, license, linecard-hardware, supervisor-hardware, syslog-group-port, system, and test.
<b>Configuration</b>	Specifies events related to configurations.
<b>Diagnostic</b>	Specifies events related to diagnostics.
<b>EEM</b>	Specifies events related to EEM.
<b>Environmental</b>	Specifies events related to power, fan, temperature related events.
<b>Inventory</b>	Specifies events related to the inventory status.
<b>License</b>	Specifies events related to license.
<b>Linecard-Hardware</b>	Specifies events related to line card hardware.
<b>Supervisor-Hardware</b>	Specifies events related to the supervisor module.
<b>Syslog-group-port</b>	Specifies events related to syslog messages filed by port manager.
<b>System</b>	Specifies events related to software.
<b>Test</b>	Specifies events related to tests.
<b>user-def-cmd</b> <i>cli_command</i>	Configures a valid CLI command for the alert group.

## Defaults

None

## Command Modes

Call home configuration

## Supported User Roles

network-admin  
vdc-admin

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

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

**Examples** This example shows how to add the **show ip routing** command to the configuration alert group:

```
switch# config t
switch(config)# callhome
switch(config-callhome)# alert-group Configuration user-def-cmd "show ip routing"
```

Related Commands	Command	Description
	<b>callhome</b>	Enters the Call home configuration mode.
	<b>callhome distribute</b>	Enables CFS distribution of the Call home configuration.
	<b>show callhome destination-profile</b> <i>name</i>	Displays one or more Call home destination profiles.







## B Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter B.

# blink

To blink the LED on the system, use the **blink** command. To restore the default LED state, use the **no** form of this command.


**Note**

Beginning with Cisco NX-OS Release 4.1(2), the **blink** command is not available in Cisco NX-OS software. Use the **locator-led** command for this function.

```
blink { chassis | fan f-number | module slot | powersupply ps-number | xbar x-number }
```

```
no blink { chassis | fan f-number | module slot | powersupply ps-number | xbar x-number }
```

**Syntax Description**

<b>chassis</b>	Blinks the chassis LED.
<b>fan</b> <i>f-number</i>	Blinks the LED that represents the configured fan number. The range depends on the platform. Use ? to see the range.
<b>module</b> <i>slot</i>	Blinks the module LED. The range depends on the platform. Use ? to see the range.
<b>powersupply</b> <i>ps-number</i>	Blinks the power supply LED. The range depends on the platform. Use ? to see the range.
<b>xbar</b> <i>x-number</i>	Blinks the xbar module LED. The range depends on the platform. Use ? to see the range.

**Defaults**

None

**Command Modes**

Any command mode

**Supported User Roles**

network-admin  
network-operator  
vdc-admin  
vdc-operator

**Command History**

Release	Modification
4.0(1)	This command was introduced.

**Usage Guidelines**

Use the **blink** command to flash the LED on a component in the system. You can use this blinking LED to identify the component to an administrator in the data center.

This command does not require a license.

---

**Examples**

This example blinks the LED for module 4:

```
switch# blink module 4
```

---

**Related Commands**

Command	Description
<b>show locator-led status</b>	Displays the status of locator LEDs on the system.

# bloggerd log-dump

To enable threshold-based log dumps on a per application, per virtual device context (VDC), per module, or on a switch-wide basis, use the **bloggerd log-dump** command. To disable threshold-based log dumps, use the **no** form of this command.

**bloggerd log-dump** { **all** | **module** *module-number* **sap** *sap-number* [**vdc** *vdc-number* | **vdc-all**] | **sap** *sap-number* [**vdc** *vdc-number* | **vdc-all**] }

**no bloggerd log-dump** { **all** | **module** *module-number* **sap** *sap-number* [**vdc** *vdc-number* | **vdc-all**] | **sap** *sap-number* [**vdc** *vdc-number* | **vdc-all**] }

## Syntax Description

<b>all</b>	Enables a log dump for all services across all modules on the device.
<b>module</b> <i>module-number</i>	Enables a log dump for the specific module. The range for the <i>module number</i> argument is from 1 to 18.
<b>sap</b> <i>sap-number</i>	Enables a log dump for a specific Service Access Point (SAP). The range for the <i>sap-number</i> argument is from 0 to 65536. A value of 0 enables a log dump of all SAPs.
<b>vdc</b> <i>vdc-number</i>	(Optional) Enables a log dump for the specific VDC. The range for the <i>vdc-number</i> argument is from 1 to 5.
<b>vdc-all</b>	(Optional) Enables a log dump for the SAP on all VDCs on the device.

## Defaults

A threshold-based log dump is enabled for the default VDC.

## Command Modes

Any command mode

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
6.2(2)	This command was introduced.

## Usage Guidelines

You can use the **bloggerd log-dump** command to prevent application logs from rolling over and becoming lost. You can enable threshold-based log dumps on a per application, per VDC, per module, or on a switch-wide basis to ensure that application logs are saved into files just before a rollover.

Once the logs are dumped, you can configure them to be transferred to a more persistent location (either an external log server or to the active supervisor module's logflash device) using the **bloggerd log transfer** command. All collected logs are in binary format and must be parsed into ASCII format using DeBlogger.

**Note**

We recommend that you use BloggerD only with TAC supervision.

This command does not require a license.

**Examples**

This example shows how to enable threshold-based log dumps on a device-wide basis:

```
switch(config)# bloggerd log-dump all  
Sending Enable Request to Bloggerd  
Bloggerd Log Dump Successfully enabled
```

**Related Commands**

Command	Description
<b>bloggerd log-transfer</b>	Enables the transfer of application logs.
<b>bloggerd parse log-buffer</b>	Parses the log buffers using DeBlogger.

# bloggerd log-transfer

To enable the transfer of application logs to an external log server or a logflash device, use the **bloggerd log-transfer** command. To disable the transfer of application logs, use the **no** form of this command.

**bloggerd log-transfer** {*ip-address tftp-path-name* | **logflash**}

**no bloggerd log-transfer**

Syntax Description		
	<i>ip-address</i>	IP address of the logging server.
	<i>tftp-path-name</i>	Name of the TFTP server path.
	<b>logflash</b>	Enables all log files to be transferred to to the active supervisor module's logflash device.

**Defaults** None

**Command Modes** Global configuration mode (config)

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	6.2(2)	This command was introduced.

**Usage Guidelines** The **bloggerd log-transfer** command allows you to configure the transfer of application logs to a more persistent location (either an external log server or to the active supervisor module's logflash device). All collected logs are in binary format and must be parsed into ASCII format using DeBlogger.



**Note**

We recommend that you use BloggerD only with TAC supervision.

This command does not require a license.

**Examples** This example shows how to enable a log dump and transfer of log files on the device:

```
switch(config)# bloggerd log-dump all
Sending Enable Request to Bloggerd
Bloggerd Log Dump Successfully enabled
switch(config)# bloggerd log-transfer 10.10.10.1 /cisco_blogger/
```

Related Commands	Command	Description
	<b>bloggerd log-dump</b>	Enables threshold-based log dumps.
	<b>bloggerd parse log-buffer</b>	Parses the log buffers using DeBlogger.

# bloggerd parse log-buffer

To parse the log buffers from binary format to ASCII format using DeBlogger, use the **bloggerd parse log-buffer** command.

**bloggerd parse log-buffer** { **directory** *directory-path* | **file** *file-name* }

## Syntax Description

<b>directory</b> <i>directory-path</i>	Specifies the directory path of file to be parsed by DeBlogger.
<b>file</b> <i>file-name</i>	Specifies the filename of file to be parsed by DeBlogger.

## Defaults

A threshold-based log dump is enabled for the default VDC.

## Command Modes

Global configuration mode (config)

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
6.2(2)	This command was introduced.

## Usage Guidelines

DeBlogger is an external parsing framework that converts binary data into ASCII format by linking with the necessary application libraries. You can use the **bloggerd parse log-buffer** command to parse logs from binary to ASCII format.



### Note

We recommend that you use BloggerD only with TAC supervision.

This command does not require a license.



**Examples**

This example shows how to parse binary logs to ASCII format on the device:

```
switch# bloggerd parse log-buffer directory /tmp/blogger/
Parsing file: /tmp/blogger//module-5_vdc-1_spm_binary_sdwrap_app_uuid_404_inst_1
_type_0_06_15_2013_00:42:56
*****
=====
META DATA:
=====
Log Data Type: SDWRAP_LOG_DATA_TYPE_EVENT_HISTORY
Module Number: 5
VDC ID: 1
APP UUID: 0
Buffer UUID: 404
Buffer Instance: 1
```

**Related Commands**

Command	Description
<b>bloggerd log-dump</b>	Enables threshold-based log dumps.
<b>bloggerd log-transfer</b>	Enables the transfer of application logs.





# C Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter C.

# callhome

To enter the CLI Call home configuration mode, use the **callhome** command.

**callhome**

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

**Defaults** Disabled

**Command Modes** Global configuration mode

**SupportedUserRoles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to enter the Call home configuration mode:

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

Related Commands		
<b>snmp-server contact</b>	Specifies or modifies the snmp-server contact name for Call home.	
<b>email-contact</b>	Specifies the e-mail address of the person responsible for the device.	
<b>phone-contact</b>	Specifies the phone number of the person responsible for the device.	
<b>streetaddress</b>	Specifies the street address of the person responsible for the device.	
<b>contract-id</b>	Specifies the service agreement contract number for this device.	
<b>customer-id</b>	Specifies the service agreement customer number for this device.	
<b>site-id</b>	Specifies the site ID number for this device.	
<b>switch-priority</b>	Specifies the priority number for this device.	
<b>destination-profile</b>	Creates and configures a Call home destination profile.	
<b>enable</b>	Enables Call home. By default, Call home is disabled.	
<b>callhome test</b>	Sends a test message to all configured destinations.	

---

<b>callhome send</b>	Sends the specified Call home test message to all configured destinations.
<b>show callhome</b>	Displays the Call home configuration.

---

# callhome send

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

**callhome send** [**configuration** | **diagnostic**]

Syntax Description	configuration	(Optional) Sends a configuration message.
	<b>diagnostic</b>	(Optional) Sends a diagnostic message.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to send a Call home configuration message:

```
switch(config)# callhome send configuration
trying to send configuration callhome message
switch(config)#
```

Related Commands	Command	Description
	<b>callhome</b>	Enters the Call home configuration mode.
	<b>callhome test</b>	Sends a test message to all configured Call home destinations.
	<b>show callhome</b>	Displays the Call home configuration.

# callhome test

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

```
callhome test {inventory}
```

<b>Syntax Description</b>	<b>inventory</b> Sends a dummy callhome inventory to all configured Call home destinations.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to send a Call home test message:
-----------------	--

```
switch(config)# callhome test  
trying to send test callhome message  
switch(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>callhome</b>	Enters the Call home configuration mode.
	<b>callhome send</b>	Sends a configuration or diagnostic message to all configured Call home destinations.
	<b>show callhome</b>	Displays the Call home configuration.

# cdp advertise

To configure the Cisco Discovery Protocol (CDP) version supported by the device, use the **cdp advertise** command. To remove the CDP configuration, use the **no** form of this command.

```
cdp advertise {v1 | v2}
```

```
no cdp advertise [v1 | v2]
```

Syntax Description	v1	Specifies CDP Version 1.
	v2	Specifies CDP Version 2.

**Defaults** None

**Command Modes** Global configuration mode (config)  
 if-ethernet-all configuration (config-if-ethernet-all)  
 if-gig-ether configuration (config-if-gig-ether)  
 if-eth-base (config-if-eth-base)  
 if-mgmt-ether (config-if-mgmt-ether)

**SupportedUserRoles** network-admin  
 vdc-admin

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

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

**Examples** This example shows how to configure the CDP version:

```
switch(config)# cdp advertise v2
switch(config)
```

This example shows how to remove the CDP configuration:

```
switch(config)# no cdp advertise v2
switch(config)
```

Related Commands	Command	Description
	<b>cdp enable</b>	Enables CDP on an interface.



# cdp enable

To enable Cisco Discovery Protocol (CDP) on an interface, use the **cdp enable** command. To disable CDP, use the **no** form of this command.

**cdp enable**

**no cdp enable**

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

**Defaults** None

**Command Modes** Global configuration mode (config)

**Supported User Roles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to enable CDP on an interface:

```
switch(config)# cdp enable
switch(config)#
```

This example shows how to disable CDP on an interface:

```
switch(config)# no cdp enable
```

Related Commands	Command	Description
	<b>cdp advertise</b>	Configures the CDP version supported by the device.

# cdp format device-id

To configure a device ID format for Cisco Discovery Protocol (CDP), use the **cdp format device-id** command. To remove the device ID format, use the **no** form of this command.

**cdp format device-id** { **mac-address** | **serial-number** | **system-name** }

**no cdp format device-id** { **mac-address** | **serial-number** | **system-name** }

Syntax Description	Parameter	Description
	<b>mac-address</b>	Specifies the MAC-address of the chassis.
	<b>serial-number</b>	Specifies the chassis serial number or Organizationally Unique Identifier (OUI).
	<b>system-name</b>	Specifies the system name. The default is fully qualified domain name.

**Defaults** None

**Command Modes** Global configuration mode (config)

**Supported User Roles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to configure a device ID format for CDP:

```
switch(config)# cdp format device-id mac-address
switch(config)#
```

This example shows how to remove the device ID format:

```
switch(config)# no cdp format device-id mac-address
switch(config)#
```

Related Commands	Command	Description
	<b>cdp enable</b>	Configures a device ID format for CDP.

# cdp holdtime

To configure the time that Cisco Discovery Protocol (CDP) holds onto neighbor information before refreshing it, use the **cdp holdtime** command. To remove the CDP hold time, use the **no** form of this command.

**cdp holdtime** *seconds*

**no cdp holdtime** *seconds*

Syntax Description	<i>seconds</i>	Hold time in seconds. The range is from 10 to 255.
--------------------	----------------	--

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

Command Modes	Global configuration mode (config)
---------------	------------------------------------

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

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

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

Examples	This example shows how to configure a time that CDP holds onto neighbor information:
----------	--

```
switch(config)# cdp holdtime 30
switch(config)#
```

This example shows how to remove the CDP hold time:

```
switch(config)# no cdp holdtime 30
switch(config)#
```

Related Commands	Command	Description
	<b>cdp timer</b>	Configures the CDP refresh time interval.

# cdp timer

To configure the Cisco Discovery Protocol (CDP) refresh time interval, use the **cdp timer** command. To remove the CDP refresh time interval configuration, use the **no** form of this command.

**cdp timer** *seconds*

**no cdp timer** *seconds*

<b>Syntax Description</b>	<i>seconds</i> Time interval in seconds. The range is from 5 to 254.				
<b>Defaults</b>	None				
<b>Command Modes</b>	Global configuration mode (config)				
<b>Supported User Roles</b>	network-admin vdc-admin				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
<b>Usage Guidelines</b>	This command does not require a license.				
<b>Examples</b>	<p>This example shows how to configure the CDP refresh time interval:</p> <pre>switch(config)# cdp timer 45 switch(config)#</pre> <p>This example shows how to remove the CDP refresh time interval:</p> <pre>switch(config)# no cdp timer 45 switch(config)#</pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>cdp holdtime</b></td> <td>Configures the time that CDP holds onto neighbor information before refreshing it.</td> </tr> </tbody> </table>	Command	Description	<b>cdp holdtime</b>	Configures the time that CDP holds onto neighbor information before refreshing it.
Command	Description				
<b>cdp holdtime</b>	Configures the time that CDP holds onto neighbor information before refreshing it.				

# cfs distribute

To globally enable Cisco Fabric Services (CFS) distribution for the device, use the **cfs distribute** command. To disable CFS distribution, use the **no** form of this command. To remove the CFS configuration, use the **no** form of this command.

**cfs distribute**

**no cfs distribute**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.1(2)	This command was introduced.

## Usage Guidelines

This command does not require a license.

In order to distribute configuration information, CFS distribution must be enabled for both the device and the application.

CFS is enabled by default for the device. All devices in the fabric must have CFS enabled or they do not receive distributions.

If CFS distribution is disabled for an application, that application does not distribute any configuration and it does not accept a distribution from other devices in the fabric.

## Examples

This example shows how to enable CFS distribution:

```
switch(config)# cfs distribute
```

## Related Commands

<b>show cfs status</b>	Displays the CFS distribution status.
<b>role distribute</b>	Enables CFS to distribute role configurations.
<b>show application_name status</b>	Displays the status of the specified application, including whether CFS distribution is enabled for the application.
<b>cfs region</b>	Specifies a region for limiting the CFS distribution scope.

# cfs eth

To globally configure the device to use Ethernet to distribute changes for all Cisco Fabric Services (CFS)-enabled applications, use the **cfs eth** command. To remove the CFS configuration, use the **no** form of this command.

**cfs eth { distribute }**

**no cfs eth distribute**

## Syntax Description

<b>distribute</b>	Enables CFS distribution over Ethernet.
-------------------	---

## Defaults

None

## Command Modes

Global configuration mode (config)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.1(2)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure the device to use Ethernet to distribute changes for all CFS-enabled applications:

```
switch(config)# cfs eth distribute
switch(config)#
```

This example shows how to remove the CFS configuration:

```
switch(config)# no cfs eth distribute
This will prevent CFS from distributing over Ethernet network.
Are you sure? (y/n) n
switch(config)#
```

## Related Commands

Command	Description
<b>cfs distribute</b>	Globally enables CFS distribution for the device.
<b>show cfs status</b>	Displays the CFS distribution status.

# cfs ipv4

To globally configure the device to use IPv4 to distribute changes for all Cisco Fabric Services (CFS)-enabled applications, use the **cfs ipv4** command. To remove the CFS configuration, use the **no** form of this command.

**cfs ipv4 [mcast | distribute]**

**no cfs ipv4 [mcast | distribute]**

## Syntax Description

<b>mcast</b>	(Optional) Configures the IPv4 multicast address over which configuration changes are distributed.
<b>distribute</b>	(Optional) Configures the device to use IPv4 to distribute changes in CFS-enabled applications.

## Defaults

The default IPv4 multicast address is 239.255.70.83.

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.1(2)	This command was introduced.

## Usage Guidelines

This command does not require a license.

CFS cannot distribute over both IPv4 and IPv6 from the same device.

In order to distribute configuration information, CFS distribution must be enabled for both the device and the application.

CFS is enabled by default for the device. All devices in the fabric must have CFS enabled or they do not receive distributions.

If CFS distribution is disabled for an application, that application does not distribute any configuration and it does not accept a distribution from other devices in the fabric.

CFS over IP must be disabled before you can change the multicast address.

## Examples

This example shows how to first disable CFS distribution over IPv4 and then configure the IPv4 multicast address over which configuration changes are distributed:

```
switch(config)# no cfs ipv4 distribute
This will prevent CFS from distributing over IPv4 network.
```

```

Are you sure? (y/n) [n] y

switch(config)# cfs ipv4 mcast-address 239.255.1.1

Distribution over this IP type will be affected

Change multicast address for CFS-IP ?

Are you sure? (y/n) [n] y

```

**Related Commands**

<b>cfs distribute</b>	Globally enables CFS distribution for the device.
<b>cfs</b>	Specifies a CFS distribution mode.
<b>show cfs status</b>	Displays the CFS distribution status.
<i>application_name</i> <b>distribute</b>	Enables distribution for the specified application, such as RADIUS.
<b>show application_name status</b>	Displays the status of the specified application, such as RADIUS, including whether CFS distribution is enabled for the application.



# cfs region

To create a Cisco Fabric Services (CFS) region that limits the distribution scope of an application, use the **cfs region** command. To remove the region or the application, use the **no** form of this command.

**cfs region** *region\_id*

*application\_name*

**no cfs region**

**no** *application\_name*

## Syntax Description

<i>region_id</i>	CFS region that is identified by numbers 0 through 200. Region 0 is the default region and it contains every device in the fabric that is not assigned to another region. You can configure region number 1 through 200.
<i>application_name</i>	Application that you assign to the specified region for CFS distribution.

## Defaults

The default region ID is 0.

## Command Modes

Global configuration mode  
CFS region configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.1(2)	This command was introduced.

## Usage Guidelines

If a feature is moved, that is, assigned to a new region, its scope is restricted to that region; it ignores all other regions for distribution or merging purposes.

You can set up a CFS region to distribute configurations for multiple applications. However, on a given device, only one CFS region at a time can distribute the configuration for a given application.

Once you assign an application to a CFS region, its configuration cannot be distributed within another CFS region.

If you remove an application from a region, and do not assign it into a different region, it is added to the default region, region 0.

If you attempt to add an application to the same region more than once, the following message appears:

```
Application already present in the same region.
```

In order to distribute configuration information, CFS distribution must be enabled for both the device and the application.

CFS is enabled by default for the device. All devices in the fabric must have CFS enabled or they do not receive distributions.

If CFS distribution is disabled for an application, then that application does not distribute any configuration and it does not accept a distribution from other devices in the fabric.

This command does not require a license.

## Examples

This example shows how to create region 4 and add the NTP application to it. When you create a region, the CLI places you into region configuration mode for that region, where you can then add an application.

```
switch(config)# cfs region 4
switch(config-cfs-region)# callhome
switch(config-cfs-region)# show cfs region brief
```

```
-----
Region      Application  Enabled
-----
4           ntp         no
4           callhome   no
6           igmp       yes
6           radius     no
```

```
switch(config-cfs-region)#
```

## Related Commands

<b>show cfs region</b>	Displays the CFS distribution region(s) configured for the device.
<b>show cfs status</b>	Displays the CFS distribution status.
<i>application_name</i> <b>distribute</b>	Enables distribution for the specified application, such as NTP.
<b>show <i>application_name</i> status</b>	Displays the status of the specified application, such as NTP, including whether CFS distribution is enabled for the application.

# check logflash

To check the compactFlash, use the **check logflash** command.

**check logflash [bad-blocks]**

<b>Syntax Description</b>	<b>bad-blocks</b> (Optional) Finds bad blocks in compactFlash.				
<b>Defaults</b>	None				
<b>Command Modes</b>	Any command mode				
<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(3)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(3)	This command was introduced.
Release	Modification				
4.0(3)	This command was introduced.				
<b>Usage Guidelines</b>	This command does not require a license.				
<b>Examples</b>	<p>This example shows how to check compactFlash:</p> <pre>switch# <b>check logflash</b></pre>				

# checkpoint

To configure the rollback checkpoint, use the **checkpoint** command. To delete the checkpoint, use the **no** form of this command.

**checkpoint** {*name* | **description** *description* | **file** *name*}

**no checkpoint** *name*

Syntax Description		
<b>name</b>	(Optional) Checkpoint name used in the checkpoint database. The name can be any alphanumeric string up to 80 characters but cannot contain spaces.	
<b>description</b> <i>description</i>	(Optional) Specifies the checkpoint description for the given checkpoint. The description can contain up to 80 alphanumeric characters, including spaces.	
<b>file</b> <i>name</i>	(Optional) Specifies the filename used to save the checkpoint.	

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** If you use the **checkpoint** command without a name, Cisco NX-OS creates the file with the name auto-x, where x is a decimal number that increases each time you create an unnamed checkpoint file.

This command does not require a license.

**Examples** This example shows how to configure the rollback checkpoint:

```
switch# checkpoint stable
switch#
```

This example shows how to delete the checkpoint file:

```
switch# no checkpoint stable
```

```
switch#
```

**Related Commands**

Command	Description
<b>clear checkpoint database</b>	Displays the contents of the checkpoint file.

# clear callhome session

To clear a Call home Cisco Fabric Services (CFS) distribution session, use the **clear callhome session** command.

## clear callhome session

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to clear a Call home CFS distribution session:

```
switch(config)# clear callhome session
```

Related Commands	Command	Description
	<b>callhome</b>	Enters the Call home configuration mode.
	<b>callhome send</b>	Sends a configuration or diagnostic message to all configured Call home destinations.
	<b>show callhome</b>	Displays the Call home configuration.

# clear cdp

To clear Cisco Discovery Protocol (CDP) statistics on an interface, use the **clear cdp** command.

```
clear cdp {counters [interface interface] | table [interface interface]}
```

Syntax Description	counters	Clears CDP counters on all interfaces.
	<b>interface</b> <i>interface</i>	(Optional) Clears CDP counters on an interface.
	<b>table</b>	Clears CDP cache on all interfaces.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to clear CDP statistics on an interface:

```
switch(config)# clear cdp counters
switch(config)#
```

Related Commands	Command	Description
	<b>enable cdp</b>	Enables CDP on an interface.

# clear checkpoint database

To delete all checkpoint files in the database, use the **clear checkpoint database** command.

## clear checkpoint database

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to clear the checkpoint database:

```
switch# clear checkpoint database
Processing the Request... Please Wait
..... Done
switch#
```

Related Commands	Command	Description
	<b>show checkpoint</b>	Displays the contents of the checkpoint file.



# clear cores

To clear the core files, use the **clear cores** command.

**clear cores** [**archive**]

<b>Syntax Description</b>	<b>archive</b> (Optional) Clears the core file on the logflash file system.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>show system cores</b> command to display information about the core files. This command does not require a license.
-------------------------	---

<b>Examples</b>	This example shows how to clear the core file:
-----------------	--

```
switch# clear cores
```

This example shows how to clear the core on the logflash file system:

```
switch# clear cores archive
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show system cores</b>	Displays the core filename.
	<b>system cores</b>	Configures the core filename.

# clear flow exporter

To clear the statistics for a Flexible NetFlow flow exporter, use the **clear flow exporter** command.

```
clear flow exporter { name exporter-name | exporter-name }
```

## Syntax Description

<b>name</b>	Specifies the name of a flow exporter.
<i>exporter-name</i>	Name of an existing flow exporter.

## Defaults

None

## Command Modes

Any command mode

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

You must have already enabled traffic monitoring with Flexible NetFlow using an exporter before you can use the **clear flow exporter** command.

This command does not require a license.

## Examples

This example clears the statistics for the flow exporter named NFC-DC-PHOENIX:

```
switch# clear flow exporter name NFC-DC-PHOENIX
switch#
```

## Related Commands

Command	Description
<b>clear flow exporter</b>	Clears the statistics for exporters.
<b>flow exporter</b>	Creates a flow exporter.
<b>show flow exporter</b>	Displays flow exporter status and statistics.

# clear flow monitor

To clear a Flexible NetFlow flow monitor, flow monitor cache, or flow monitor statistics and to force the export of the data in the flow monitor cache, use the **clear flow monitor** command.

```
clear flow monitor { name monitor-name | monitor-name } [cache [force-export] | statistics]
```

## Syntax Description

<b>name</b>	Specifies the name of a flow monitor.
<i>monitor-name</i>	Name of an existing flow monitor.
<b>cache</b>	(Optional) Clears the flow monitor cache information.
<b>force-export</b>	(Optional) Forces the export of the flow monitor cache statistics.
<b>statistics</b>	(Optional) Clears the flow monitor statistics.

## Defaults

None

## Command Modes

Any command mode

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

You must enable Flexible NetFlow monitor before you can use the **clear flow monitor** command.

Use the **clear flow monitor monitor-name cache** command to remove all entries from the flow monitor cache. These entries will not be exported and the data gathered in the cache is lost.

The statistics for the cleared cache entries are maintained.

Use the **clear flow monitor monitor-name force-export** command to remove all entries from the flow monitor cache and exports them to all flow exporters that are assigned to the flow monitor. This process can result in a short term increase in the CPU utilization.



### Caution

Be careful when you use the **clear flow monitor monitor-name force-export** command because using this command might cause a short-term increase in the CPU utilization.

Use the **clear flow monitor monitor-name statistics** command to clear the statistics and cache entries for this flow monitor.

The Current entries statistic is not cleared because this statistic indicates how many entries are in the cache.

This command does not require a license.

### Examples

This example shows how to clear the statistics and cache entries for the flow monitor named NFC-DC-PHOENIX:

```
switch# clear flow monitor name NFC-DC-PHOENIX
switch#
```

This example shows how to clear the statistics and cache entries for the flow monitor named NFC-DC-PHOENIX and forces an export:

```
switch# clear flow monitor NFC-DC-PHOENIX force-export
switch#
```

This example shows how to clear the cache for the flow monitor named NFC-DC-PHOENIX and forces an export:

```
switch# clear flow monitor NFC-DC-PHOENIX cache force-export
switch#
```

This example shows how to clear the statistics for the flow monitor named NFC-DC-PHOENIX:

```
switch# clear flow monitor NFC-DC-PHOENIX statistics
switch#
```

### Related Commands

Command	Description
<b>clear flow monitor</b>	Clears the flow monitor.
<b>flow monitor</b>	Creates a flow monitor.
<b>show flow sw-monitor</b>	Displays flow monitor status and statistics.

# clear hardware flow ip

To clear the NetFlow hardware IP flow, use the **clear hardware flow ip** command.

```
clear hardware flow ip [{{ vdc vdc_id } | { monitor name } | { profile profile-id } | { vlan vlan-id } |
{ interface if-type if-number }}] [instance inst] [force-export] [module num]
```

Syntax Description		
<b>vdc</b> <i>vdc_id</i>	Specifies the VDC. The range is from 1 to 16.	
<b>monitor</b> <i>name</i>	Specifies the name of the NetFlow flow monitor. The monitor name can be any case-sensitive, alphanumeric string up to 64 characters.	
<b>profile</b> <i>profile-id</i>	Specifies the name of the flow profile. The range is from 1 to 31.	
<b>vlan</b> <i>vlan-id</i>	Specifies the VLAN. The range is from 1 to 4094.	
<b>interface</b>	Specifies the interface.	
<i>if-type</i>	Interface type. For more information, use the question mark (?) online help function.	
<i>if-number</i>	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.	
<b>instance</b> <i>inst</i>	(Optional) Specifies the EARL instance. The EARL instance can be any alphanumeric string up to 32 characters.	
<b>force-export</b>	(Optional) Forces data to be exported to the collector prior to the clear operation.	
<b>module</b> <i>num</i>	(Optional) Specifies the module.	

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to clear the NetFlow hardware IP flow:

```
switch(config)# clear hardware flow ip module 8 ethernet 2/1
switch(config)#
```

■ clear hardware flow ip

Related Commands	Command	Description
	<b>show hardware flow</b> <b>{ip   ipv6}</b>	Displays information about NetFlow hardware IP / IPV6 flows.

# clear logging ip access-list cache

To clear all the entries from the Optimized ACL Logging (OAL) cache and send them to the syslog, use the **clear logging ip access-list cache** command.

## clear logging ip access-list cache

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to clear all the entries from the OAL cache and send them to the syslog:

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

Related Commands	Command	Description
	show logging ip access-list	Displays the logging status for IP access lists.

# clear logging logfile

To clear messages from the logging file, use the **clear logging logfile** command.

## clear logging logfile

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to clear messages from the logging file:

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

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



# 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.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**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.

# clear logging onboard

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

```
clear logging onboard [counter-stats] [environmental-history] [error-stats] [exception-log]
[interrupt-stats] [module num] [obfl-log] [stack-trace]
```

Syntax Description	
<b>counter-stats</b>	(Optional) Clears the OBFL counter statistics.
<b>environmental-history</b>	(Optional) Clears the OBFL environmental history.
<b>error-stats</b>	(Optional) Clears the OBFL error statistics.
<b>exception-log</b>	(Optional) Clears the OBFL exception log entries.
<b>interrupt-stats</b>	(Optional) Clears the OBFL interrupt statistics.
<b>module num</b>	(Optional) Clears the OBFL information for a specific module.
<b>obfl-log</b>	(Optional) Clears the OBFL (boot-up/uptime/device-version/obfl-history).
<b>stack-trace</b>	(Optional) Clears the OBFL stack trace entries.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(2)	Added the <b>counter-stats</b> keyword.

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

**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 error statistics:

```
switch# clear logging onboard error-stats
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 interrupt statistics:

```
switch# clear logging onboard interrupt-stats
switch#
```

This example shows how to clear the OBFL information for a specific module:

```
switch# clear logging onboard module 2
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
<b>hw-module logging onboard</b>	Enables OBFL based on the error type.
<b>show logging onboard</b>	Displays onboard failure logs.

# 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.

---

**Defaults** None

---

**Command Modes** Any command mode

---

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

---

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

---



---

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

---

**Examples** This example shows how to clear the current logging session:

```
switch# clear logging session
switch#
```

---

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

---

# 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.

---

**Defaults** None

---

**Command Modes** Any command mode

---

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.2(1)	This command was introduced.

---

---

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

---

**Examples** This example shows how to clear the NTP session:

```
switch(config)# clear ntp session
```

# clear ntp statistics

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

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

Syntax Description	all-peers	Clears statistics for all NTP peers.
	io	Clears IO statistics.
	local	Clears local statistics.
	memory	Clears memory statistics.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to clear statistics for all NTP peers:

```
switch(config)# clear ntp statistics all-peers
```

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

# clear nvram

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

**clear nvram**

---

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

---

**Defaults** None

---

**Command Modes** Any command mode

---

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

---

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

---

---

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

---

**Examples** This example shows how to clear NVRAM:  
switch(config)# **clear nvram**

# clear platform flow ip

To clear NetFlow hardware IPv4 entries, use the **clear platform flow ip** command.

```
clear platform flow ip [type] [force-export] [module mod-num]
```

Syntax Description		
<i>type</i>	(Optional) Type of entry to clear. See the “Usage Guidelines” section for valid values.	
<b>force-export</b>	(Optional) Specifies a forced export of the cleared data to a collector.	
<b>module</b> <i>mod-num</i>	(Optional) Specifies a module. The ranges for the module number depends on the chassis used.	

**Defaults** If you do not specify the type, all types are cleared.

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to specify a forced export of the cleared data to a collector:

```
switch# clear platform flow ip forced-export
switch#
```

This example shows how to clear the NetFlow statistics for a module:

```
switch# clear platform flow ip module 2
switch#
```



**Related Commands**

<b>Command</b>	<b>Description</b>
<b>flow exporter</b>	Creates a flow exporter.
<b>clear flow monitor</b>	Clears the flow monitor.
<b>flow monitor</b>	Creates a flow monitor.
<b>show flow sw-monitor</b>	Displays flow monitor status and statistics.

# clear processes log archive

To delete a log file on a log flash, use the **clear processes log archive** command.

**clear processes log archive** [*file file-number*]

<b>Syntax Description</b>	<b>file file-number</b> (Optional) Specifies to delete a log file on a log flash.	
<b>Defaults</b>	None	
<b>Command Modes</b>	Any command mode	
<b>Supported User Roles</b>	network-admin network-operator vdc-admin vdc-operator	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.
<b>Usage Guidelines</b>	This command does not require a license.	
<b>Examples</b>	This example shows how to delete a log file on a log flash:	
	<pre>switch(config)# clear processes log archive switch(config)#</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show processes log</b>	Displays the contents of the process log.

# 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 PTP packet counters for all PTP interfaces.
	<b>interface ethernet slot / port</b>	Clears PTP packet counters for an Ethernet interface. The slot number is from 1 to 255 and the port number is from 1 to 128.

**Defaults** None

**Command Modes** EXEC mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	7.3(0)DX(1)	This command was introduced.

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

**Examples** This example shows how to clear PTP counters for all PTP interfaces:

```
switch(config)# clear ptp counters all
switch(config)#
```

Related Commands	Command	Description
	<b>show ptp counters</b>	Displays PTP specific packet counters for all Ethernet interfaces or for a specified interface.

# clear rmon

To delete the Remote Network Monitoring (RMON) tables from a simple network management protocol (SNMP) notification, use the **clear rmon** command.

```
clear rmon {alarms | events | hcalarms | all-alarms}
```

Syntax Description	alarms	Clears all 32-bit alarms.
	events	Clears the RMON log and also clears the RMON event table.
	hcalarms	Clears all 64-bit RMON alarms.
	all-alarms	Clears all 32-bit and 64-bit RMON alarms.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to delete RMON tables:

```
switch(config)# clear rmon alarms
switch(config)#
```

Related Commands	Command	Description
	clear snmp counters	Deletes SNMP counters.

# clear session state name

To clear the state information for a session, use the **clear session state name** command.

**clear session state name** *name*

<b>Syntax Description</b>	<i>name</i>	Name of the session. The name can be any case-sensitive, alphanumeric string up to 63 characters.
---------------------------	-------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>Supported User Roles</b>	network-admin network-operator vdc-admin vdc-operator
-----------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to clear the internal state for a configuration session:  switch# <b>clear session state name myACLs</b>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show configuration session</b>	Displays information about the configuration sessions.

# clear snmp counters

To delete Simple Network Management Protocol (SNMP) counters, use the **clear snmp counters** command.

**clear snmp counters**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to delete SNMP counters:

```
switch(config)# clear snmp counters
switch(config)#
```

To see if the counters have been reset, use the show command:

```
switch(config)# show snmp
sys contact:
sys location: anyplace, Anywhere

0 SNMP packets input
  0 Bad SNMP versions
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors
  0 No such name errors
```

```
0 Bad values errors
0 General errors
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show snmp sessions</b>	Displays information about SNMP sessions.

# clear snmp hostconfig

To delete the Simple Network Management Protocol (SNMP) host configuration, use the **clear snmp hostconfig** command.

**clear snmp hostconfig**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to delete the SNMP host configuration:

```
switch(config)# clear snmp hostconfig
switch(config)#
```

Related Commands	Command	Description
	show snmp sessions	Displays SNMP sessions.
	clear snmp counters	Deletes SNMP counters.



# clear system reset-reason

To clear the device reset-reason history, use the **clear system reset-reason** command.

**clear system reset-reason**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to clear the device reset-reason history:

```
switch# clear system reset-reason
```

Related Commands	Command	Description
	show system reset-reason	Displays the device reset-reason history.

# collect counter

To configure the number of bytes or packets in a flow as a nonkey field and collect the counter values (number of bytes or packets seen) for a Flexible NetFlow flow record, use the **collect counter** command. To disable the use of the number of bytes or packets in a flow (counters) as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

**collect counter** {bytes [long] | packets [long]}

**no collect counter** {bytes [long] | packets [long]}

Syntax Description		
<b>bytes</b>		Configures the number of bytes seen in a flow as a nonkey field and collects the total number of bytes from the flow.
<b>long</b>		(Optional) Collects the total number of bytes from the flow using a 64-bit counter.
<b>packets</b>		Configures the number of bytes seen in a flow as a nonkey field and collects the total number of packets from the flow.

**Defaults** This command is not enabled by default.

**Command Modes** Flow record configuration

**SupportedUserRoles** network-admin  
vdc-admin

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

**Usage Guidelines** The Flexible NetFlow commands that start with **collect** are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases, the values for nonkey fields are taken from only the first packet in the flow.

Use the **collect counter packets** command to configure a 32-bit counter that is incremented for each packet seen in the flow. For extremely long flow it is possible for this counter to wrap when it reaches the limit of 4 billion or more packets. When the flow monitor detects a scenario that could cause a wrap, the flow monitor with a normal cache type exports the flow and starts a new flow.

Use the **collect counter packets long** command to configure a 64-bit counter that is incremented for each packet seen in the flow. It is unlikely that a 64-bit counter will ever wrap.

This command does not require a license.

**Examples**

This example shows how to enable collecting the total number of bytes from the flows as a nonkey field:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# collect counter bytes
```

This example shows how to enable collecting the total number of bytes from the flows as a nonkey field using a 64 bit counter:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# collect counter bytes long
```

This example shows how to enable collecting the total number of packets from the flows as a nonkey field:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# collect counter packets
```

This example shows how to enable collecting the total number of packets from the flows as a nonkey field using a 64-bit counter:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# collect counter packets long
```

**Related Commands**

Command	Description
<b>collect counter</b>	Configures the counters as a nonkey field and collects the counter values.
<b>collect flow</b>	Configures flow identifying fields as nonkey fields and collects their values.
<b>collect interface</b>	Configures the input and/or output interface as a nonkey field and collects the values.
<b>collect ipv4</b>	Configures an IPv4 field as a nonkey field and collects the value in it.
<b>collect routing</b>	Configures a routing attribute as a nonkey field and collects the value of the field.
<b>collect timestamp</b>	Configures the time stamp fields as nonkey fields and collects the values.
<b>collect transport</b>	Configures a transport layer field as a nonkey field and collects the values.
<b>debug flow record</b>	Enables debugging output for flow records.
<b>flow record</b>	Creates a flow record.
<b>match flow</b>	Configures one or more of the flow fields as key fields.
<b>match interface</b>	Configures the direction that traffic flows in respect to an interface (interface field) as a key field.
<b>match ipv4</b>	Configures one or more of the IPv4 fields as a key field.
<b>match routing</b>	Configures one or more of the routing fields as a key field.
<b>match timestamp</b>	Configures a time stamp field as a key field.
<b>match transport</b>	Configures one or more of the transport fields as key fields.
<b>show flow record</b>	Displays the flow record status and statistics.

# collect flow

To configure the flow direction or the flow sampler ID number as a nonkey field and collect their values for a Flexible NetFlow flow record, use the **collect flow** command. To disable the use of the flow direction or the flow sampler ID number as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

**collect flow** { **direction** | **sampler** }

**no collect flow** { **direction** | **sampler** }

## Syntax Description

<b>direction</b>	Configures the flow direction as a nonkey field and collects the direction that the flow was monitored in.
<b>sampler</b>	Configures the flow sampler ID as a nonkey field and collects the ID of the sampler that is assigned to the flow monitor.

## Defaults

This command is not enabled by default.

## Command Modes

Flow record configuration

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

The Flexible NetFlow commands that start with **collect** are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases, the values for nonkey fields are taken from only the first packet in the flow.

Use the **collect flow direction** command to indicate the direction of the flow. Use this command when you configure a single flow monitor for input and output flows and to find and eliminate flows that are being monitored twice: once on input and once on output.

Use the **collect flow sampler** command to collect the ID of the flow sampler that is used to monitor the flow. Use this command when more than one flow sampler is being used with different sampling rates. The **option sampler-table** command exports option records with mappings of the flow sampler ID to the sampling rate so that the collector can calculate the scaled counters for each flow.

This command does not require a license.

**Examples**

This example shows how to configure the direction of the flow nonkey that was monitored as a nonkey field:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# collect flow direction
```

This example shows how to configure an ID of the flow sampler that is assigned to the flow as a nonkey field and collects the ID of the flow sampler:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# collect flow sampler
```

**Related Commands**

Command	Description
<b>collect counter</b>	Configures the counters as a nonkey field and collects the counter values.
<b>collect flow</b>	Configures flow identifying fields as nonkey fields and collects their values.
<b>collect interface</b>	Configures the input and/or output interface as a nonkey field and collects the values.
<b>collect ipv4</b>	Configures an IPv4 field as a nonkey field and collects the value in it.
<b>collect routing</b>	Configures a routing attribute as a nonkey field and collects the value of the field.
<b>collect timestamp</b>	Configures the times tamp fields as nonkey fields and collects the values.
<b>collect transport</b>	Configures a transport layer field as a nonkey field and collects the values.
<b>flow record</b>	Creates a flow record.
<b>match flow</b>	Configures one or more of the flow fields as key fields.
<b>match interface</b>	Configures the direction that traffic flows in respect to an interface (interface field) as a key field.
<b>match ipv4</b>	Configures one or more of the IPv4 fields as a key field.
<b>match routing</b>	Configures one or more of the routing fields as a key field.
<b>match timestamp</b>	Configures a time stamp field as a key field.
<b>match transport</b>	Configures one or more of the transport fields as key fields.
<b>show flow record</b>	Displays the flow record status and statistics.

# collect interface

To configure the input or output interface as a nonkey field and collect the values for a Flexible NetFlow flow record, use the **collect interface** command. To disable the use of the input or output interface as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

```
collect interface {input | output}
```

```
no collect interface {input | output}
```

## Syntax Description

<b>input</b>	Configures the input interface as a nonkey field and collects the input interface from the flows.
<b>output</b>	Configures the output interface as a nonkey field and collects the output interface from the flows.

## Defaults

This command is not enabled by default.

## Command Modes

Flow record configuration

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

The Flexible NetFlow commands that start with **collect** are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases, the values for nonkey fields are taken from only the first packet in the flow.

This command does not require a license.

## Examples

This example shows how to configure the input interface as a nonkey field and collect the input interface value:

```
switch(config)# flow record FLOW-RECORD-1  
switch(config-flow-record)# collect interface input
```

This example shows how to configure the output interface as a nonkey field and collect the output interface value:

```
switch(config)# flow record FLOW-RECORD-1  
switch(config-flow-record)# collect interface output
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>collect counter</b>	Configures the counters as a nonkey field and collects the counter values.
<b>collect flow</b>	Configures flow identifying fields as nonkey fields and collects their values.
<b>collect interface</b>	Configures the input or output interface as a nonkey field and collects the values.
<b>collect ipv4</b>	Configures an IPv4 field as a nonkey field and collects the value in it.
<b>collect routing</b>	Configures a routing attribute as a nonkey field and collects the value of the field.
<b>collect timestamp</b>	Configures the time stamp fields as a nonkey field and collects the values.
<b>collect transport</b>	Configures a transport layer field as a nonkey field and collects the values.
<b>flow record</b>	Creates a flow record.
<b>match flow</b>	Configures one or more of the flow fields as key fields.
<b>match interface</b>	Configures the direction that traffic flows in respect to an interface (interface field) as a key field.
<b>match ipv4</b>	Configures one or more of the IPv4 fields as a key field.
<b>match routing</b>	Configures one or more of the routing fields as a key field.
<b>match timestamp</b>	Configures a time stamp field as a key field.
<b>match transport</b>	Configures one or more of the transport fields as key fields.
<b>show flow record</b>	Displays the flow record status and statistics.

# collect routing

To configure a routing attribute as a nonkey field and collect the value of the field for a Flexible NetFlow flow record, use the **collect routing** command. To disable the use of a routing attribute as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

```
collect routing {{ destination | source } as [peer] | traffic-index | forwarding-status | next-hop
address ipv4 [bgp]}
```

```
no collect routing {{ destination | source } as [peer] | traffic-index | forwarding-status | next-hop
address ipv4 [bgp]}
```

## Syntax Description

<b>destination</b>	Configures one or more of the destination routing attributes fields as a nonkey field and collects the values from the flows.
<b>source</b>	Configures one or more of the source routing attributes fields as a nonkey field and collects the values from the flows.
<b>as</b>	Configures the destination AS field as a nonkey field and collects the value in the AS field from the flows.
<b>peer</b>	(Optional) Configures the destination AS number of the peer network as a nonkey field and collects the value of the AS number of the peer network from the flows.
<b>traffic-index</b>	Configures the Border Gateway Protocol (BGP) source or destination traffic index as a nonkey field and collects the value of the BGP destination traffic index from the flows.
<b>forwarding-status</b>	Collects the forwarding status of the packet and triggers the collection of flows denied by Access Control List (ACL) entries.
<b>next-hop address ipv4</b>	Configures the next-hop value as a nonkey field and collects information regarding the next-hop from the flows.
<b>bgp</b>	(Optional) Configures the IP address of the next hop BGP network as a nonkey field and collects the value of the IP address of the BGP next-hop network from the flows.

## Defaults

This command is not enabled by default.

## Command Modes

Flow record configuration

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.



**Usage Guidelines**

The Flexible NetFlow commands that start with **collect** are used to configure nonkey fields for the flow monitor record and to capture the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases, the values for nonkey fields are taken from only the first packet in the flow.

Use the **collect routing source as** [*peer*] command to collect the 16-bit AS number based on a lookup of the router's routing table using the source IP address. The optional **peer** keyword provides the expected next network, not the originating network.

**Note**

The the 16-bit AS number is based on how packets are routed back from this router and the value might

not be accurate for asymmetrical routes.

Use the **collect routing destination as** [*peer*] command to collect the 16-bit AS number based on a lookup of the router's routing table using the destination IP address. The optional **peer** keyword provides the expected next network, not the destination network.

Use the **collect routing source traffic-index** command to collect the traffic index field based on the source AS for this flow. The traffic-index field is a value that is propagated through BGP.

Use the **collect routing forwarding-status** command to collect a field to indicate if the packets were successfully forwarded. The field is in two parts and may be up to 4 bytes in length. At this time, only the status field is used:

```

+-----+
| S | Reason | |
| t | codes  |
|   | a | or   |
| t | flags  |
| u |         |
| s |         |
+-----+
0 1 2 3 4 5 6 7

```

Status:

00b=Unknown, 01b = Forwarded, 10b = Dropped, 11b = Consumed

This command does not require a license.

**Examples**

This example shows how to configure the 16-bit AS number based on a lookup of the router's routing table using the source IP address as a nonkey field and collects the 16-bit AS number value:

```

switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# collect routing source as

```

This example shows how to configure the 16-bit AS number based on a lookup of the router's routing table using the destination IP address as a nonkey field and collects the 16-bit AS number value:

```

switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# collect routing destination as

```

This example shows how to configure the value in the traffic index field based on the source AS for a flow as a nonkey field and collects the value in the traffic index field value:

```

switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# collect routing source traffic-index

```

This example shows how to configure the forwarding status as a nonkey field and collects the forwarding status value:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# collect routing forwarding-status
```

#### Related Commands

Command	Description
<b>collect counter</b>	Configures the counters as a nonkey field and collects the counter values.
<b>collect flow</b>	Configures flow identifying fields as nonkey fields and collects their values.
<b>collect interface</b>	Configures the input or output interface as a nonkey field and collects the values.
<b>collect ipv4</b>	Configures an IPv4 field as a nonkey field and collects the value in it.
<b>collect routing</b>	Configures a routing attribute as a nonkey field and collects the value of the field.
<b>collect timestamp</b>	Configures the times tamp fields as a nonkey field and collects the values.
<b>collect transport</b>	Configures a transport layer field as a nonkey field and collects the values.
<b>flow record</b>	Creates a flow record.
<b>match flow</b>	Configures one or more of the flow fields as key fields.
<b>match interface</b>	Configures the direction that traffic flows in respect to an interface (interface field) as a key field.
<b>match ipv4</b>	Configures one or more of the IPv4 fields as key fields.
<b>match routing</b>	Configures one or more of the routing fields as key fields.
<b>match timestamp</b>	Configures a time stamp field as a key field.
<b>match transport</b>	Configures one or more of the transport fields as key fields.
<b>show flow record</b>	Displays the flow record status and statistics.

# collect timestamp sys-uptime

To configure the `TIMESTAMP SYS-UPTIME` field as a nonkey field and collect the values in them for a Flexible NetFlow flow record, use the **collect timestamp sys-uptime** command. To disable the use of the `TIMESTAMP SYS-UPTIME` field as a nonkey for a Flexible NetFlow flow record, use the **no** form of this command.

```
collect timestamp sys-uptime {first | last}
```

```
no collect timestamp sys-uptime {first | last}
```

Syntax Description	first	last
	Configures the sys-uptime for the time that the first packet was seen from the flows as a nonkey field and collects time stamps based on the sys-uptime for the time that the first packet was seen from the flows.	Configures the sys-uptime for the time that the last packet was seen from the flows as a nonkey field and collects time stamps based on the sys-uptime for the time that the most recent packet was seen from the flows.

**Defaults** This command is not enabled by default.

**Command Modes** Flow record configuration

**SupportedUserRoles** network-admin  
vdc-admin

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

**Usage Guidelines** The Flexible NetFlow commands that start with **collect** are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases, the values for nonkey fields are taken from only the first packet in the flow.

This command does not require a license.

**Examples** This example shows how to configure timestamps based on the sys-uptime for the time that the first packet was seen from the flows as a nonkey field and collects the sys-uptime for the time that the first packet was seen from the flows:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# collect timestamp sys-uptime first
```

This example shows how to configure timestamps based on the sys-uptime for the time that the most recent packet was seen from the flows as a nonkey field and collects the sys-uptime for the time that the most recent packet was seen from the flows:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# collect timestamp sys-uptime last
```

### Related Commands

Command	Description
<b>collect counter</b>	Configures the counters as a nonkey field and collects the counter values.
<b>collect flow</b>	Configures flow identifying fields as nonkey fields and collects their values.
<b>collect interface</b>	Configures the input or output interface as a nonkey field and collects the values.
<b>collect ipv4</b>	Configures an IPv4 field as a nonkey field and collects the value in it.
<b>collect routing</b>	Configures a routing attribute as a nonkey field and collects the value of the field.
<b>collect timestamp</b>	Configures the time stamp fields as a nonkey field and collects the values.
<b>collect transport</b>	Configures a transport layer field as a nonkey field and collects the values.
<b>flow record</b>	Creates a flow record.
<b>match flow</b>	Configures one or more of the flow fields as key fields.
<b>match interface</b>	Configures the direction that traffic flows in respect to an interface (interface field) as a key field.
<b>match ipv4</b>	Configures one or more of the IPv4 fields as key fields.
<b>match routing</b>	Configures one or more of the routing fields as key fields.
<b>match timestamp</b>	Configures a time stamp field as a key field.
<b>match transport</b>	Configures one or more of the transport fields as key fields.
<b>show flow record</b>	Displays the flow record status and statistics.

# collect transport tcp flags

To configure a Transmission Control Protocol (TCP) field as a nonkey field and collect the value in it for a Flexible NetFlow flow record, use the **collect transport tcp flags** command. To disable the use of a TCP field as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

**collect transport tcp flags**

**no collect transport tcp flags**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command is not enabled by default.

## Command Modes

Flow record configuration

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

The Flexible NetFlow commands that start with **collect** are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases, the values for nonkey fields are taken from only the first packet in the flow.

This command does not require a license.

## Examples

This example shows how to configure the TCP flags as a nonkey field:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# collect transport tcp flags
```

## Related Commands

Command	Description
<b>collect counter</b>	Configures the counters as a nonkey field and collects the counter values.
<b>collect flow</b>	Configures flow identifying fields as nonkey fields and collects their values.
<b>collect interface</b>	Configures the input or output interface as a nonkey field and collects the values.

<b>Command</b>	<b>Description</b>
<b>collect ipv4</b>	Configures an IPv4 field as a nonkey field and collects the value in it.
<b>collect routing</b>	Configures a routing attribute as a nonkey field and collects the value of the field.
<b>collect timestamp</b>	Configures the timestamp fields as nonkey fields and collects the values.
<b>collect transport</b>	Configures a transport layer field as a nonkey field and collects the values.
<b>flow record</b>	Creates a flow record.
<b>match flow</b>	Configures one or more of the flow fields as key fields.
<b>match interface</b>	Configures the direction that traffic flows in respect to an interface (interface field) as a key field.
<b>match ipv4</b>	Configures one or more of the IPv4 fields as key fields.
<b>match routing</b>	Configures one or more of the routing fields as key fields.
<b>match timestamp</b>	Configures a time stamp field as a key field.
<b>match transport</b>	Configures one or more of the transport fields as key fields.
<b>show flow record</b>	Displays the flow record status and statistics.

# commit (Call home)

To distribute a Cisco Fabric Services (CFS) configuration, use the **commit** command.

**commit**

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

**Defaults** None

**Command Modes** Call home configuration

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

**Usage Guidelines** The **commit** command results in the distribution of the CFS configuration to the running configuration of all CFS-enabled devices in the fabric.

You can only use the **commit** command on the specific device where the fabric lock was acquired.

Configuration changes that have not been committed yet (still saved as a working copy) are not in the running configuration and do not display in the output of **show** commands.

An empty commit is allowed to distribute a current configuration if you want to make sure that all devices are synchronized.

This command does not require a license.

**Examples** This example shows how to commit a CFS configuration and verify that the commit was successful:

```
switch(config-callhome)# commit
switch(config-callhome)# show callhome session status
Last Action Time Stamp      : Tue Dec 23 11:15:02 2008
Last Action                  : Commit
Last Action Result           : Success
Last Action Failure Reason  : none
```

Related Commands	Command	Description
	<b>abort</b>	Deletes the CFS session.
	<b>show cfs application</b>	Displays the applications that are currently CFS-enabled.
	<b>show <i>application_name</i> session status</b>	Displays information about the CFS configuration session status for an application.



# commit (Session Manager)

To validate and apply the commands in the Session Manager configuration session, use the **commit** command.

**commit** [**verbose**]

<b>Syntax Description</b>	<b>verbose</b> (Optional) Displays a detailed version of the results of the <b>commit</b> command.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Session configuration
----------------------	-----------------------

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	<p>The <b>commit</b> command results in a validation of the entire Session Manager configuration, and, if valid, the configuration is applied to the device.</p> <p>This command does not require a license.</p>
-------------------------	--

<b>Examples</b>	This example shows how to commit a Session Manager configuration:
-----------------	---

```
switch# config session ACL_tcp_in
Config Session started, Session ID is 1
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-s)# verify
Verification Successful
switch(config-s)# commit
Commit Successful
switch#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>abort</b>	Deletes the session and exists session configuration mode.
	<b>exit</b>	Exits session configuration mode without committing the commands.
	<b>show configuration session</b>	Displays information about the Session Manager configuration session.

# configure maintenance profile

To enter a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile, use the **configure maintenance profile** command. To delete the existing maintenance mode profile or normal mode profile, use the **no** form of this command. Starting with Cisco NX-OS Release 7.3(0)D1(1), we recommend not using the **configure profile [maintenance-mode | normal-mode] type admin** command and we strongly recommend using the **configure maintenance profile [maintenance-mode | normal-mode]** command.

**configure maintenance profile [maintenance-mode | normal-mode]**

**no configure maintenance profile [maintenance-mode | normal-mode]**

## Syntax Description

**maintenance-mod e** Enters the maintenance profile configuration session for a maintenance mode profile.

**normal-mode** Enters the maintenance profile configuration session for a normal mode profile.

## Defaults

None

## Command Modes

Privileged EXEC (#)

Global configuration mode (config)

## SupportedUserRoles

network-admin

vdc-admin

network-operator

vdc-operator

## Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to enter a maintenance profile configuration session for a maintenance mode profile:

```
switch# configure maintenance profile maintenance-mode
```

```
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom profile always for maintenance mode.
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
switch(config-mm-profile)#
```

This example shows how to enter a maintenance profile configuration session for a normal mode profile:

```
switch# configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)#
```

This example shows how to delete a maintenance profile:

```
switch# no configure maintenance profile maintenance-mode
Maintenance mode profile maintenance-mode successfully deleted
Enter configuration commands, one per line. End with CNTL/Z.
Exit maintenance profile mode.
```

### Related Commands

Command	Description
<b>show run mmode</b>	Displays the currently running maintenance profile configuration on a switch.
<b>show system mode</b>	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
<b>system mode maintenance always-use-custom-profile</b>	Applies the existing custom maintenance-mode profile and prevents creation of auto-generated maintenance-mode profile.
<b>system mode maintenance on-reload reset-reason</b>	Boots the switch into maintenance-mode automatically in the event of a specified system crash.
<b>system mode maintenance shutdown</b>	Shuts down all protocols and interfaces except the management interface (by using the <b>shutdown</b> command and not the default <b>isolate</b> command).
<b>system mode maintenance timeout</b>	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

# configure session

To create or modify an access control list (ACL) configuration session with the Session Manager feature, use the **configure session** command.

**configure session** *name*

Syntax Description	<i>name</i>	Name of the session. The name can be any case-sensitive, alphanumeric string up to 63 characters.
--------------------	-------------	---

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

Command Modes	Any command mode
---------------	------------------

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

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

Usage Guidelines	This command does not require a license. Session Manager supports only the ACL feature.
------------------	--

**Examples** This example shows how to create an ACL configuration session:

```
switch# configure session myACLs
switch(config-s)#
```

Related Commands	Command	Description
	<b>show configuration session</b>	Displays information about the Session Manager configuration sessions.

# configure profile maintenance-mode type admin

To enter the configuration session for the maintenance mode profile file, use the **configure profile maintenance-mode type admin** command.

**configure profile maintenance-mode type admin**

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

**Defaults** None.

**Command Modes** Profile configuration.

Command History	Release	Modification
	7.2.0	This command was introduced.

**Examples** This example shows how to create a maintenance mode profile file:

```
switch# configure terminal
switch(config)# configure profile maintenance-mode type admin
switch(config-profile)# router ospf 100
switch(config-profile-router)# max-metric router-lsa
switch(config-profile-router)# exit
switch(config-profile)# router eigrp 101
switch(config-profile-router)# max-metric router-lsa
switch(config-profile-router)# exit
switch(config-profile)# router isis 102
switch(config-profile-router)# max-metric router-lsa
switch(config-profile-router)# set-overload-bit always
switch(config-profile-router)# exit
switch(config-profile)# router bgp 103
switch(config-profile-router)# max-metric router-lsa
switch(config-profile-router)# exit
switch(config-profile)# vpc domain 20
switch(config-profile-router)# max-metric router-lsa
switch(config-profile-router)# exit
switch(config-profile)# system interface shutdown
switch(config-profile)# end
Exit configure profile mode.
switch#
```

# configure profile normal-mode type admin

To enter the configuration session for the normal mode profile file, use the **configure profile normal-mode type admin** command.

**configure profile normal-mode type admin**

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

**Defaults** None.

**Command Modes** Profile configuration.

Command History	Release	Modification
		This command was introduced.

## Usage Guidelines

**Examples** This example shows how to create a normal mode profile file:

```
switch# configure terminal
switch(config)# configure profile normal-mode type admin
switch(config-profile)# router ospf 100
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router eigrp 101
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router isis 102
switch(config-profile-router)# no shutdown
switch(config-profile-router)# no set-overload-bit always
switch(config-profile-router)# exit
switch(config-profile)# router bgp 103
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# vpc domain 20
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# no system interface shutdown
switch(config-profile)# end
Exit configure profile mode.
switch#
```

# contract-id

To specify a service agreement contract ID in Call home, use the **contract-id** command. To remove it, use the **no** form of this command.

**contract-id** *contract\_id\_number*

**no contract-id**

Syntax Description	
<i>contract_id_number</i>	Contract number for this device from the service agreement. The contract number can be up to 255 alphanumeric characters in free format.

Defaults	
	None

Command Modes	
	Call home configuration

SupportedUserRoles	
	network-admin vdc-admin

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

Usage Guidelines	
	This command does not require a license.

Examples	
	This example shows how to configure a service agreement contract ID in Call home: <pre>switch(config-callhome)# <b>contract-id Contract5678</b></pre>

Related Commands	Command	Description
	<b>callhome</b>	Places you into Call home configuration mode.
	<b>email-contact</b>	Specifies the e-mail address of the person responsible for the device.
	<b>phone-contact</b>	Specifies the phone number of the person responsible for the device.
	<b>streetaddress</b>	Specifies the street address of the person responsible for the device.
	<b>customer-id</b>	Specifies the service agreement customer number for this device.
	<b>site-id</b>	Specifies the site ID number for this device.
	<b>switch-priority</b>	Specifies the priority number for this device.
	<b>show callhome</b>	Displays the Call home configuration.





```
tx-performance [poll-interval poll-interval {absolute rising-threshold rising-threshold
event event-id [falling-threshold falling-threshold event event-id] | delta rising-threshold
rising-threshold event event-id [falling-threshold falling-threshold event event-id]}]}
```

Syntax Description		
<b>invalid-crc</b>		Configures the invalid-crc counter.
<i>poll-interval</i>		(Optional) Poll interval for counter in seconds. The range is from 0 to 2147483647.
<b>absolute</b>		Specifies the absolute type threshold.
<b>rising-threshold</b>		Configures the rising-threshold value.
<i>rising-threshold</i>		Rising-threshold limit. The range is from 0 to 18446744073709551615.
<b>event</b>		Configures the rising-threshold event.
<i>event-id</i>		Event ID from the event configuration. The range is from 1 to 65535.
<b>falling-threshold</b>		(Optional) Configures the falling-threshold value.
<i>falling-threshold</i>		(Optional) Falling-threshold limit. The range is from -2147483648 to 2147483647.
<b>delta</b>		(Optional) Specifies the delta type threshold.
<b>invalid-words</b>		Configures the invalid-words counter.
<b>link-loss</b>		Configures the link-loss counter.
<b>protocol-error</b>		Configures the protocol-error counter.
<b>rx-performance</b>		Configures the ingress (rx) performance counter.
<b>signal-loss</b>		Configures the signal-loss counter.
<b>sync-loss</b>		Configures the sync-loss counter.
<b>tx-performance</b>		Configures the egress (tx) performance counter.

**Defaults** None

**Command Modes** Port-monitor configuration (config-port-monitor)

**Supported User Roles** network-admin  
vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to configure an SNMP counter:

```
switch(config) port-monitor name PM1
switch(config-port-monitor)# counter invalid-crc poll-interval 30 absolute
rising-threshold 10000000 event 100
```

```
switch(config-port-monitor)#
```

This example shows how to remove an SNMP counter configuration:

```
switch(config)# no counter invalid-crc poll-interval 30 absolute rising-threshold 10000000
event 100
switch(config-port-monitor)#
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>monitor counter</b>	Configures a monitor counter.

---

# customer-id

To specify a service agreement customer ID in Call home, use the **customer-id** command. To remove it, use the **no** form of this command.

**customer-id** *contract\_id\_number*

**no customer-id**

<b>Syntax Description</b>	<i>contract_id_number</i>	Customer number for this device from the service agreement. The customer number can be up to 255 alphanumeric characters in free format.
---------------------------	---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Call home configuration
----------------------	-------------------------

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to configure a service agreement customer ID in Call home: <pre>switch(config-callhome)# <b>customer-id</b> Customer123456</pre>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>callhome</b>	Places you into Call home configuration mode.
	<b>email-contact</b>	Specifies the e-mail address of the person responsible for the device.
	<b>phone-contact</b>	Specifies the phone number of the person responsible for the device.
	<b>streetaddress</b>	Specifies the street address of the person responsible for the device.
	<b>contract-id</b>	Specifies the service agreement contract number for this device.
	<b>site-id</b>	Specifies the site ID number for this device.
	<b>switch-priority</b>	Specifies the priority number for this device.
	<b>show callhome</b>	Displays the Call home configuration.





## D Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter D.

## description (EEM)

To add a description to an Embedded Event Manager (EEM) applet, use the **description** command. To remove the description, use the **no** form of this command.

**description** *description*

**no description**

Syntax Description	<i>description</i>	Comment or a description that is added to an EEM applet.
--------------------	--------------------	--

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

Command Modes	Embedded event manager
---------------	------------------------

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

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

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

Examples	This example shows how to add a description to an EEM applet:
----------	---

```
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)# description "counter policy for acme"
switch(config-applet)#
```

Related Commands	Command	Description
	<b>show event manager policy</b>	Displays information about the configured EEM policy.

# description (NetFlow record)

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

**description** *line*

**no description** [*line*]

Syntax Description	<i>line</i>	Description string. The string can have a maximum of 63 alphanumeric characters.
--------------------	-------------	--

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

Command Modes	NetFlow record configuration (config-flow-record)
---------------	---

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

Command History	Release	Modification
	4.0(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 NetFlow record:
----------	--

```
switch(config)# flow record NetFlow-Record-1
switch(config-flow-record)# description Custom-Flow-Record-1
switch(config-flow-record)#
```

Examples	This example shows how to remove the description:
----------	---

```
switch(config-flow-record)# no description
```

Related Commands	Command	Description
	<b>show flow record</b>	Displays information about NetFlow records.

# description (NetFlow monitor)

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

**description** *line*

**no description** [*line*]

Syntax Description	<i>line</i>	Description string. The string can have a maximum of 63 alphanumeric characters.
--------------------	-------------	--

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

Command Modes	NetFlow monitor configuration (config-flow-monitor)
---------------	---

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

Command History	Release	Modification
	4.0(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 NetFlow monitor:
----------	---

```
switch(config)# flow monitor NetFlow-Monitor-1
switch(config-flow-monitor)# description Custom-Monitor-1
switch(config-flow-monitor)#
```

This example shows how to remove the description:

```
switch(config-flow-monitor)# no description
```

Related Commands	Command	Description
	<b>show flow sw-monitor</b>	Displays information about NetFlow monitors.



## description (NetFlow exporter)

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

**description** *line*

**no description** [*line*]

Syntax Description	<i>line</i>	Description string. The string can have a maximum of 63 alphanumeric characters.
--------------------	-------------	--

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

Command Modes	NetFlow exporter configuration (config-flow-exporter)
---------------	---

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

Command History	Release	Modification
	4.0(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 NetFlow exporter:
----------	--

```
switch(config)# flow export Netflow-Exporter-1
switch(config-flow-exporter)# description Custom-Exporter-1
switch(config-flow-exporter)
```

This example shows how to remove the description:

```
switch(config-flow-exporter)# no description
switch(config-flow-exporter)
```

Related Commands	Command	Description
	<b>show flow exporter</b>	Displays information about NetFlow exporters.

## description (NetFlow sampler)

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

**description** *line*

**no description** [*line*]

Syntax Description	<i>line</i>	Description string. The string can have a maximum of 63 alphanumeric characters.
--------------------	-------------	--

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

Command Modes	NetFlow sampler configuration (config-flow-sampler)
---------------	---

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

Command History	Release	Modification
	4.0(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 NetFlow sampler:
----------	---

```
switch(config)# sampler Netflow-Sampler-1
switch(config-flow-sampler)# description Custom-Sampler-1
switch(config-flow-sampler)#
```

This example shows how to remove the description:

```
switch(config-flow-sampler)# no description
```

Related Commands	Command	Description
	<b>show sampler</b>	Displays information about NetFlow samplers.

# description (SPAN)

To add a description to an Ethernet Switched Port Analyzer (SPAN) session for analyzing traffic between ports, use the **description** command. To remove the description, use the **no** form of this command.

**description** *description*

**no description**

Syntax Description	<i>description</i>	Comment or a description of up to 32 characters that is added to a SPAN session.
--------------------	--------------------	--

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

Command Modes	Monitor configuration (config-monitor)
---------------	--

Supported User Roles	network-admin vdc-admin
----------------------	----------------------------

Command History	Release	Modification
	4.0(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 SPAN session:
----------	--

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# description span_session_3
```

Related Commands	Command	Description
	<b>monitor session</b>	Places you into the Monitor configuration mode for configuring a SPAN session.
	<b>show monitor session</b>	Displays the specified SPAN or ERSPAN session configuration.

# destination

To specify the destination for a NetFlow exporter, use the **destination** command. To remove a destination, use the **no** form of this command.

```
destination {ipaddr | ipv6addr} [use-vrf vrf_name]
```

```
no destination [{ipaddr | ipv6addr} [use-vrf vrf_name]
```

Syntax Description	
<i>ipaddr</i>	Destination IP address for a collector.
<i>ipv6addr</i>	Destination IPv6 address for a collector.
<b>use-vrf</b> <i>vrf_name</i>	(Optional) Specifies the Virtual Routing and Forwarding (VRF) label.

Defaults	
	None

Command Modes	
	NetFlow exporter configuration (config-flow-exporter)

SupportedUserRoles	
	network-admin vdc-admin

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

Usage Guidelines	
	This command does not require a license.

Examples	
	This example shows how to specify the destination for a NetFlow exporter:

```
switch(config)# Flow exporter NetFlow-Exporter-1  
switch(config-flow-exporter)# destination 192.168.11.2  
switch(config-flow-exporter)#
```

This example shows how to remove the destination:

```
switch(config-flow-exporter)# no destination
```

Related Commands	Command	Description
	<b>show flow exporter</b>	Displays information about NetFlow exporters.

# destination interface (SPAN)

To add a destination interface to an Ethernet Switched Port Analyzer (SPAN) session for analyzing traffic between ports, use the **destination interface** command. To remove the destination, use the **no** form of this command.

**destination interface** { **ethernet** *number* | **port-channel** *number* }

**no destination interface** { **ethernet** *number* | **port-channel** *number* }

## Syntax Description

<b>ethernet</b> <i>number</i>	Specifies the destination Ethernet interface slot number for the specified SPAN session. Source packets are copied from this destination. The range is from 1 through 10.
<b>port-channel</b> <i>number</i>	Specifies the destination port channel interface for the specified SPAN session. Source packets are copied from this destination. The range is from 1 through 4096.

## Defaults

None

## Command Modes

Monitor configuration (config-monitor)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to add a destination to a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7
```

## Related Commands

Command	Description
<b>monitor session</b>	Places you into the Monitor configuration mode for configuring a SPAN session.

<b>Command</b>	<b>Description</b>
<b>show monitor session</b>	Displays the specified SPAN or ERSPAN session configuration.
<b>description</b>	Adds a comment or a description of up to 32 characters to a SPAN session.

# destination-profile

To create and name a destination profile for Call home, use the **destination-profile** command. To remove a destination profile, use the **no** form of this command.

**destination-profile** *profile\_name*

**no destination-profile** *profile\_name*

Syntax Description	
	<i>profile_name</i> User-defined destination profile name.

Defaults	
	None

Command Modes	
	Call home configuration (config-callhome)

SupportedUserRoles	
	network-admin vdc-admin

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

Usage Guidelines	
	<p>Cisco NX-OS includes the following predefined destination profiles:</p> <ul style="list-style-type: none"> <li>• CiscoTAC-1—Supports the Cisco-TAC alert group in XML message format. This profile is preconfigured with the callhome@cisco.com e-mail contact, maximum message size, and message severity level 0. You cannot change any of the default information for this profile.</li> <li>• full-text-destination—Supports the full text message format.</li> <li>• short-text-destination—Supports the short text message format.</li> </ul> <p>This command does not require a license.</p>

Examples	
	<p>This example shows how to create the Call home destination profile named Noc101:</p>

```
switch(config)# callhome
switch(config-callhome)# destination-profile Noc101
```

This example shows how to remove the Call home Noc101 destination profile:

```
switch(config)# callhome
switch(config-callhome)# no destination-profile Noc101
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show callhome destination-profile name</b>	Displays the specified Call home destination profile.
<b>show callhome</b>	Displays the Call home configuration.



# destination-profile alert-group

To specify which alerts a Call home destination will receive, use the **destination-profile alert-group** command. To remove an alert group, use the **no** form of this command.

**destination-profile** *profile\_name* **alert-group** { **All** | **Configuration** | **Diagnostic** | **EEM** | **Cisco-TAC** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test** }

**no destination-profile** *profile\_name* **alert-group** { **All** | **Configuration** | **Diagnostic** | **EEM** | **Cisco-TAC** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test** }

## Syntax Description

<i>profile_name</i>	User-defined Call home destination profile name.
<b>alert-group</b>	Adds an alert group to the specified Call home destination profile.
<b>All</b>	Specifies that the Call home destination profile receives all callhome messages.
<b>Configuration</b>	Specifies that the Call home destination profile is notified of events related to configuration.
<b>Diagnostic</b>	Specifies that the Call home destination profile is notified of events related to the diagnostic.
<b>EEM</b>	Specifies that the Call home destination profile is notified of EEM events.
<b>Cisco-TAC</b>	Specifies that the Call home destination profile is notified of events that are meant for Cisco TAC only.
<b>Environmental</b>	Specifies that the Call home destination profile is notified of events related to power, fan, and temperature.
<b>Inventory</b>	Specifies that the Call home destination profile is notified of inventory status events.
<b>License</b>	Specifies that the Call home destination profile is notified of events related to licensing.
<b>Linecard-Hardware</b>	Specifies that the Call home destination profile is notified of line card-related events.
<b>Supervisor-Hardware</b>	Specifies that the Call home destination profile is notified of supervisor-related events.
<b>Syslog-group-port</b>	Specifies that the Call home destination profile is notified of events related to syslog messages filed by port manager.
<b>System</b>	Specifies that the Call home destination profile is notified of software-related events.
<b>Test</b>	Specifies that the Call home destination profile is notified of user-generated test events.

## Defaults

None

## Command Modes

Call home configuration (config-callhome)

## destination-profile alert-group

**SupportedUserRoles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to specify that the destination profile receives all Call home messages:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# destination-profile Noc101 alert-group All
switch(config-callhome)# show callhome destination-profile profile Noc101

Noc101 destination profile information
maximum message size:2500000
message format:XML
message-level:0
email addresses configured:

alert groups configured:
all
```

Related Commands	Command	Description
	<b>show callhome</b>	Displays the Call home configuration.

# destination-profile email-addr

To specify an e-mail address for a Call home destination, use the **destination-profile email-addr** command. To remove an e-mail address, use the **no** form of this command.

**destination-profile** *profile-name* **email-addr** *email-address*

**no destination-profile** *profile-name* **email-addr** *email-address*

<b>Syntax Description</b>	<i>profile-name</i>	Name you have given the Call home destination profile where the e-mail address is to be added.
	<b>email-addr</b> <i>email-address</i>	Specifies the e-mail address to be added to the Call home destination profile.

**Defaults** None

**Command Modes** Call home configuration (config-callhome)

**SupportedUserRoles** network-admin  
vdc-admin

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

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

**Examples** This example shows how to specify an e-mail address for a Call home destination:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# destination-profile Noc101 email-addr jdoe@callhome.com
switch(config-callhome)# show callhome destination-profile profile Noc101

Noc101 destination profile information
maximum message size:2500000
message format:XML
message-level:0
email addresses configured:
jdoe@callhome.com

alert groups configured:
all
```

■ destination-profile email-addr

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show callhome</b>	Displays the Call home configuration.

# destination-profile format

To specify a message format for sending messages to a Call home destination, use the **destination-profile format** command.

```
destination-profile profile_name format { full-txt | short-txt | XML }
```

## Syntax Description

<i>profile_name</i>	Name you have given the Call home destination profile where the message format is to be specified.
<b>format</b>	Establishes a format for sending Call home messages to the specified destination (XML is the default).
<b>full-txt</b>	Specifies that messages are sent to the named Call home destination in plain text.
<b>short-txt</b>	Specifies that messages are sent to the named Call home destination in short text.
<b>XML</b>	Specifies that messages are sent to the named Call home destination in XML. XML is the default Call home message format.

## Defaults

XML

## Command Modes

Call home configuration (config-callhome)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure a message format for sending messages to a Call home destination:

```
switch(config-callhome)# destination-profile acme_destination format full-txt
```

## Related Commands

Command	Description
<b>show callhome destination-profile</b>	Displays a Call home destination profiles.
<b>show callhome</b>	Displays the Call home configuration.

## destination-profile http

To specify an HTTP or HTTPS URL for a Call home destination, use the **destination-profile http** command. To remove a URL, use the **no** form of this command.

**destination-profile** *profile-name* **http** *url*

**no destination-profile** *profile-name* **http** *url*

<b>Syntax Description</b>	<i>profile-name</i>	Name you have given the Call home destination profile.
	<b>http</b> <i>url</i>	Specifies the HTTP or HTTPS URL to be added to the Call home destination profile.
<b>Defaults</b>	None	
<b>Command Modes</b>	Call home configuration (config-callhome)	
<b>SupportedUserRoles</b>	network-admin vdc-admin	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.
<b>Usage Guidelines</b>	This command does not require a license.	
<b>Examples</b>	This example shows how to configure a URL for a Call home destination: <pre>switch(config-callhome)# destination-profile acme_destination http http://my_url.com/callhome</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show callhome destination-profile</b>	Displays a Call home destination profiles.
	<b>show callhome</b>	Displays the Call home configuration.

# destination-profile message-level

To specify a severity level for alerts that are sent to the Call home destination, use the **destination-profile message-level** command.

**destination-profile** *profile\_name* **message-level** *number*

Syntax Description	
<i>profile_name</i>	Name you have given the Call home destination profile where the message format is to be specified.
<b>message-level</b>	Specifies the severity level at which messages that are sent to the Callhome destination.
<i>number</i>	Message severity level designations that begin at the lowest urgency level 0 and progress to level 9, the most urgent. If you specify level 5, for example, all messages designated level 5 or higher are sent to the destination.

**Defaults** None

**Command Modes** Call home configuration (config-callhome)

**SupportedUserRoles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to specify that messages with a severity level 5 or higher are sent to a Call home destination:

```
switch(config-callhome)# destination-profile acme_destination message-level 5
```

Related Commands	Command	Description
	<b>show callhome destination-profile</b>	Displays a Call home destination profiles.
	<b>show callhome</b>	Displays the Call home configuration.

# destination-profile message-size

To specify a maximum allowable size for messages that are sent to a Call home destination, use the **destination-profile message-size** command.

**destination-profile** *profile\_name* **message-size** *number*

Syntax Description	
<i>profile_name</i>	Name you have given the Call home destination profile where the maximum message size is to be specified.
<b>message-size</b>	Specifies the maximum allowable size for messages sent to the specified Call home destination. The default is 2500000.
<i>number</i>	Maximum allowable size of a message sent to the specified Call home destination. The range is from 0 to 5000000.

**Defaults** 2500000

**Command Modes** Call home configuration (config-callhome)

**SupportedUserRoles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to configure a maximum message size of 100000 for messages sent to a Call home destination:

```
switch(config-callhome)# destination-profile acme_destination message-size 100000
```

Related Commands	Command	Description
	<b>show callhome destination-profile</b>	Displays a Call home destination profiles.
	<b>show callhome</b>	Displays the Call home configuration.



# destination-profile transport-method

To specify a method of transporting Call home messages to a destination, use the **destination-profile transport-method** command. To remove the transport method, use the **no** form of this command.

**destination-profile** *profile-name* **transport-method** [**email** | **http**]

**no destination-profile** *profile-name* **transport-method** [**email** | **http**]

## Syntax Description

<i>profile-name</i>	Name you have given the Call home destination profile where the transport method is to be specified.
<b>transport-method</b>	Specifies the method (email or HTTP) for sending messages to the Call home destination.
<b>email</b>	(Optional) Specifies if using e-mail to send Call home messages to the Call home destination.
<b>http</b>	(Optional) Specifies if using HTTP to send Call home messages to the Call home destination.

## Defaults

None

## Command Modes

Call home configuration (config-callhome)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to specify HTTP for transporting Call home messages to a destination:

```
switch(config-callhome)# destination-profile acme_destination transport-method http
switch(config-callhome)#
```

## Related Commands

Command	Description
<b>show callhome destination-profile</b>	Displays a Call home destination profiles.
<b>show callhome</b>	Displays the Call home configuration.

# diagnostic bootup level

To configure the diagnostic bootup level to trigger diagnostics when the device boots, use the **diagnostic bootup level** command.

**diagnostic bootup level** {bypass | complete}

Syntax Description		
	<b>bypass</b>	Specifies to not perform any bootup diagnostics.
	<b>complete</b>	Displays all bootup diagnostics. The default is complete.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to configure the diagnostic bootup level:

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

Related Commands	Command	Description
	show diagnostic bootup level	Displays the diagnostic bootup level.

# diagnostic clear result module

To clear the diagnostic test result for the specified test, use the **diagnostic clear result module** command.

**diagnostic clear result module** [**slot** | **all**] **test** {*test-id* | **all**}

Syntax Description	slot	(Optional) Specifies to clear the a diagnostic test for a specific module number. The range is from 1 to 10.
	<b>all</b>	(Optional) Displays the test result for all tests on all modules.
	<b>test</b>	Displays the diagnostic test selection.
	<i>test-id</i>	Test ID. The range is from 1 to 14.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to clear a diagnostic test result:

```
switch# diagnostic clear result module 6 test 6
```

Related Commands	Command	Description
	show diagnostic result	Displays a diagnostic test result for a specified test.

# diagnostic eem action conservative

To configure the device to take corrective action when it detects failures on the PortLoopback test, the RewriteEngineLoopback test, the SnakeLoopback test, or the StandbyFabricLoopback test, use the **diagnostic eem action conservative** command.

## diagnostic eem action conservative

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

**Defaults** None

**Command Modes** Global command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	6.2(8)	This command was introduced.

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

**Examples** This example shows how to direct the switch to take corrective action:

```
switch# diagnostic eem action conservative
```

Related Commands	Command	Description
	show event manager events action-log event-type [ gold   gold_sup_failure   gold_fabric_failure   gold_module_failure   gold_port_failure ]	Displays the recovery action history including the number of switchovers/reloads/poweroffs, timestamp, failure reason, module-id, port list, test name, testing type, and severity. This data is maintained across ungraceful reloads.

# diagnostic monitor interval module

To configure a diagnostic monitoring test interval on a module, use the **diagnostic monitor interval module** command. To remove the diagnostic monitoring test interval, use the **no** form of this command.

```
diagnostic monitor interval module module test {all | name | test-id} hour hour min min second
sec
```

```
no diagnostic monitor interval module module test {all | name | test-id}
```

## Syntax Description

<i>module</i>	Module number.
<b>test</b>	Specifies a diagnostic test.
<b>all</b>	Specifies all test IDs.
<i>name</i>	Test name.
<i>test-id</i>	Test ID number.
<b>hour</b>	Specifies the hour of the interval that the test begins.
<i>hour</i>	Hour of the interval that you specify to start the test.
<b>min</b>	Specifies the minute of the interval that the test begins.
<i>min</i>	Minute of the interval that you specify to start the test.
<b>second</b>	Specifies the second of the interval that the test begins.
<i>sec</i>	Second of the interval that you specify to start the test.

## Defaults

None

## Command Modes

Global configuration mode (config)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure a diagnostic monitoring test interval on a module:

```
switch(config)# diagnostic monitor interval module 1 test 5 hour 10 min 30 sec 0
switch(config)#
```

This example shows how to remove a diagnostic monitoring test interval from a module:

**diagnostic monitor interval module**

```
switch(config)# no diagnostic monitor interval module 1 test 5 hour 10 min 30 sec 0  
switch(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show running-config diagnostic</b>	Displays the running-configuration diagnostics.
<b>diagnostic monitor module</b>	Configures a diagnostic monitor test.

# diagnostic monitor module

To configure a diagnostic monitor test, use the **diagnostic monitor module** command. To remove a diagnostic monitor test, use the **no** form of this command.

```
diagnostic monitor module module test {all | name | test-id}
```

```
no diagnostic monitor module module test {all | name | test-id}
```

## Syntax Description

<i>module</i>	Module number.
<b>test</b>	Specifies a diagnostic test selection.
<b>all</b>	Specifies all test IDs.
<i>name</i>	Test name. The maximum number of characters is 32.
<i>test-id</i>	Test ID number.

## Defaults

None

## Command Modes

Global configuration mode (config)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure a diagnostic monitor test:

```
switch(config)# diagnostic monitor module 1 test all  
  
switch(config)#
```

This example shows how to remove a diagnostic monitor test:

```
switch(config)# no diagnostic monitor module 1 test all  
switch(config)#
```

Related Commands	Command	Description
	<b>show startup-config diagnostic</b>	Displays the startup-configuration diagnostics.
	<b>show running-config diagnostic</b>	Displays the running-configuration diagnostics.



# diagnostic ondemand action-on-failure

To configure the action to take if the on-demand test fails, use the **diagnostic ondemand action-on-failure** command.

**diagnostic ondemand action-on-failure** { **continue failure-count** *num-fails* | **stop** }

Syntax Description	continue failure-count <i>num-fails</i>	stop
	Displays the on-demand test until the test failure limit is reached. The range is from 1 to 999. The default is 1.	Stops on-demand tests immediately if a test fails.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to configure the action if the on-demand test fails:

```
switch# diagnostic ondemand action-on-failure continue failure-count 992
switch#
```

Related Commands	Command	Description
	show diagnostic ondemand	Displays information about on-demand tests.

# diagnostic ondemand iteration

To configure the number of times that the on-demand test runs, use the **diagnostic ondemand iteration** command.

**diagnostic ondemand iteration** *number*

<b>Syntax Description</b>	<i>number</i>	(Optional) Number of times that the on-demand test runs. The range is from 1 to 999. The default is 1.
---------------------------	---------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to configure the number of times that the on-demand test runs: <pre>switch# diagnostic ondemand iteration 992</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show diagnostic ondemand</b>	Displays information about on-demand tests.

# diagnostic start

To start the on-demand diagnostic test for a module, use the **diagnostic start** command.

**diagnostic start module slot test** [*test-id* | *test-name* | **all** | **non-disruptive**] [**port** *port-number* | **all**]

Syntax Description		
<i>slot</i>	(Optional)	Diagnostic start slot number. The range is from 1 to 10.
<b>test</b>		Displays the diagnostic test.
<i>test-id</i>	(Optional)	Test ID. The range is from 1 to 14.
<i>test-name</i>	(Optional)	Test name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
<b>all</b>	(Optional)	Displays all ports.
<b>non-disruptive</b>	(Optional)	Displays the nondisruptive tests.
<b>port</b>	(Optional)	Displays the port interface.
<i>port-number</i>	(Optional)	Interface port number.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to start the on-demand diagnostic test for a module:

```
switch# diagnostic start module 6 test all
```

Related Commands	Command	Description
	<b>diagnostic stop</b>	Stops on-demand diagnostics.

# diagnostic stop

To stop one or more diagnostic tests for a module, use the **diagnostic stop** command.

**diagnostic stop module** *slot test* [*test-id* | *name* | **all**]

Syntax Description		
<i>slot</i>		Slot number. The slot range is from 1 to 10.
<b>test</b>		Displays the diagnostic test.
<i>test-id</i>		(Optional) Test ID. The range is from 1 to 14.
<i>name</i>		(Optional) Test name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
<b>all</b>		(Optional) Displays the diagnostic test for all tests on all modules.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to stop one or more diagnostic tests on a module:

```
switch# diagnostic stop module 6 test all
switch#
```

Related Commands	Command	Description
	<b>diagnostic start</b>	Starts one or more diagnostic tests.

# diagnostic test simulation

To simulate a diagnostic test for a module, use the **diagnostic test simulation** command

```
diagnostic test simulation module slot test test-id [port {number | all}] {fail | random-fail | success}
```

## Syntax Description

<i>slot</i>	Diagnostic test simulation module number. The range is from 1 to the number of modules in the chassis.
<b>test</b> <i>test-id</i>	Specifies the test ID. The range is from 1 to 15.
<b>port</b>	(Optional) Specifies the interface port to display.
<i>number</i>	Interface port number.
<b>all</b>	Specifies all interface ports.
<b>fail</b>	Displays failed test results.
<b>random-fail</b>	Displays random fail test results.
<b>success</b>	Displays pass test results.

## Defaults

None

## Command Modes

Any command mode

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to simulate a test result:

```
switch# diagnostic test simulation module 2 test 2 fail  
switch#
```

Related Commands	Command	Description
	<b>diagnostic test simulation clear</b>	Clears a diagnostic test simulation.

# diagnostic test simulation clear

To clear a diagnostic test simulation for a module, use the **diagnostic test simulation clear** command

**diagnostic test simulation module** *number* **test** *test-id* **clear**

Syntax Description	module <i>number</i>	test <i>test-id</i>
	Specifies the diagnostic test simulation module number. The range is from 1 to the number of modules in the chassis.	Specifies the test ID. The range is from 1 to 15.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to clear the diagnostic test simulation:

```
switch# diagnostic test simulation module 2 test 2 clear
switch#
```

Related Commands	Command	Description
	<b>diagnostic test simulation</b>	Simulates a diagnostic test.

# distribute

To enable Cisco Fabric Service (CFS) to distribute configurations, use the **distribute** command. To disable distribution, use the **no** form of this command.

**distribute** [**radius** | **tacacs+**]

**no distribute**

## Syntax Description

<b>radius</b>	(Optional) Specifies CFS to distribute RADIUS configurations.
<b>tacacs+</b>	(Optional) Specifies CFS to distribute TACACS+ configurations.

## Defaults

None

## Command Modes

Call home configuration mode  
Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.1(2)	This command was introduced.

## Usage Guidelines

This command does not require a license.  
To enable CFS to distribute role configurations, see the **role distribute** command.

## Examples

This example shows how to enable CFS to distribute Call home configurations:

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

This example shows how to enable CFS to distribute RADIUS configurations:

```
switch(config)# distribute radius
```

This example shows how to enable CFS to distribute TACACS+ configurations:

```
switch(config)# distribute tacacs+
```



Related Commands	Command	Description
	<b>show cfs status</b>	Displays the CFS distribution status.
	<b>cfs</b>	Specifies a CFS distribution mode.
	<b>cfs region</b>	Creates a CFS distribution region that limits the distribution scope of an application.

# dscp

To specify the differentiated services code point (DSCP) for a NetFlow exporter, use the **dscp** command. To remove the DSCP parameter, use the **no** form of this command.

**dscp** *dscp*

**no dscp** [*dscp*]

<b>Syntax Description</b>	<i>dscp</i> Differentiated services code point value. The range is from 0 to 63.				
<b>Defaults</b>	None				
<b>Command Modes</b>	NetFlow exporter configuration (config-flow-exporter)				
<b>Supported User Roles</b>	network-admin vdc-admin				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
<b>Usage Guidelines</b>	This command does not require a license.				
<b>Examples</b>	<p>This example shows how to configure the DSCP parameter:</p> <pre>switch(config)# <b>Flow exporter Custom-NetFlow-Exporter-1</b> switch(config-flow-exporter)# <b>dscp 32</b> switch(config-flow-exporter)#</pre> <p>This example shows how to remove the DSCP parameter:</p> <pre>switch(config-flow-exporter)# <b>no dscp</b> switch(config-flow-exporter)</pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show flow exporter</b></td> <td>Displays information about NetFlow exporters.</td> </tr> </tbody> </table>	Command	Description	<b>show flow exporter</b>	Displays information about NetFlow exporters.
Command	Description				
<b>show flow exporter</b>	Displays information about NetFlow exporters.				



## E Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter E.

# erspan-id

To configure the flow ID for an Encapsulated Remote Switched Port Analyzer (ERSPAN)) session, use the **erspan-id** command.

**erspan-id** *flow\_id*

Syntax Description	<i>flow_id</i>	ERSPAN flow ID. The range is from 1 to 1023.
--------------------	----------------	--

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

Command Modes	config-erspan-src
---------------	-------------------

Supported User Roles	network-admin network-operator
----------------------	-----------------------------------

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

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

Examples	This example shows how to configure the flow ID for an ERSPAN session:
	<pre>switch# configure terminal switch(config)# monitor session 5 type erspan-source switch(config-erspan-src)# erspan-id 100 switch(config-erspan-src)#</pre>

Related Commands	Command	Description
	<b>ip dscp</b>	Configures the DSCP value of the packets in the ERSPAN traffic.
	<b>ip ttl</b>	Configures the IP time-to-live (TTL) value of the ERSPAN traffic.
	<b>vrf</b>	Configures the VRF for ERSPAN traffic forwarding.
	<b>monitor-session</b>	Enters the monitor configuration mode for configuring an ERSPAN or SPAN session for analyzing traffic between ports.

# ethanalyzer local interface

To capture packets to or from the supervisor or management interface, use the **ethanalyzer local interface** command. To stop packet capture, use the **no** form of this command.

```
ethanalyzer local interface { inband | mgmt } [[capture-filter capt-expression]
[capture-ring-buffer duration seconds write bootflash | files files write bootflash |
filesize kilobytes write bootflash [display-filter disp-expression] [limit-captured-frames limit]
[limit-frame-size bytes] [write location]] [brief]

no ethanalyzer local interface { inband | mgmt } [[capture-filter capt-expression]
[capture-ring-buffer duration seconds write bootflash | files files write bootflash | filesize
kilobytes write bootflash [display-filter disp-expression] [limit-captured-frames limit]
[limit-frame-size bytes] [write location]] [brief]
```

Syntax Description		
<b>inband</b>		Captures packets going between the supervisor module and the interface modules.
<b>mgmt</b>		Captures packets going to or from the mgmt0 port.
<b>capture-filter</b> <i>capt-expression</i>		(Optional) Filters the display of output based on the expression. The expression is a quoted string.
<b>capture-ring-buffer</b>		(Optional) Captures ring buffer option.
<b>duration</b>		Stop writing to the file or switch to the next file after value seconds have elapsed.
<i>seconds</i>		Duration in seconds. The range is from 0-2147483647.
<b>write</b>		Filename to save capture to.
<b>files</b>		Stop writing to capture files after value number of files were written or begin again with the first file after value number of files were written (form a ring buffer).
<i>files</i>		Number of files. The range is from 2 to 64.
<i>bootflash</i>		Specifies the bootflash file name.
<b>filesize</b>		Stop writing to a capture file or switch to the next file after it reaches a size of value kilobytes.
<i>kilobytes</i>		Size in kilobytes. The range is from 1to 65536.
<b>display-filter</b> <i>disp-expression</i>		(Optional) Filters the display of output based on the expression. The expression is a quoted string.
<b>limit-captured-frames</b> <i>limit</i>		(Optional) Configures the maximum number of frames to capture. The range is from 0 to 2147483647. The default is 100.
<b>limit-frame-size</b> <i>bytes</i>		(Optional) Captures the configured number of bytes from a frame. The range is from 64 to 65535.
<b>write</b> <i>location</i>		(Optional) Saves the captured information to the configured location. The location can be any case-sensitive, alphanumeric string up to 64 characters.
<b>brief</b>		(Optional) Displays the protocol summary of the captured packets.

## Defaults

No packets captured.

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.2(5) and 5.0(1)	Added the option <b>capture-ring-buffer</b> to the syntax description.
	4.0(1)	This command was introduced.

**Usage Guidelines** Cisco Ethalyzer is based on the Wireshark open source code.  
This command does not require a license.

**Examples** This example shows how to capture all packets on the mgmt 0 port:

```
switch# ethalyzer local interface mgmt
#
```

Related Commands	Command	Description
	<b>ethalyzer local read</b>	Reads the captured packet data from an Ethalyzer capture.

# ethalyzer local read

To read packets captured by Ethalyzer, use the **ethalyzer local read** command. To stop reading the packet capture, use the **no** form of this command.

**ethalyzer local read** *location*

**no ethalyzer local read** *location*

<b>Syntax Description</b>	<i>location</i>	Location to read captured packets from. The location can be any case-sensitive, alphanumeric string up to 64 characters.
<b>Defaults</b>	None	
<b>Command Modes</b>	Any command mode	
<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.
<b>Usage Guidelines</b>	Cisco Ethalyzer is based on the Wireshark open source code. This command does not require a license.	
<b>Examples</b>	This example shows how to capture all packets on the mgmt 0 port: switch# <b>ethalyzer local read bootflash:test-mgmt0</b> #	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ethalyzer local interface</b>	Captures packets to or from the supervisor or mgmt0 port.

# event cli

To specify the event criteria for an Embedded event manager (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 countnum] [time interval]
```

```
no event cli match regex [count countnum] [time interval]
```

Syntax Description	tag <i>tag</i>	(Optional) Identifies this specific event when multiple events are included in the policy.
	<b>match</b> <i>regex</i>	Specifies the regular expression ( <i>regex</i> ) used to perform the CLI command pattern match. The CLI command must have been successfully parsed before the pattern match is attempted. The pattern match is compared with the fully expanded CLI command string. If the expression contains embedded blanks, enclose it in double quotation marks.
	<b>count</b> <i>countnum</i>	(Optional) Specifies the number of matching occurrences before an EEM event is triggered. When a number is not specified, an EEM event is triggered after the first match. The <i>countnum</i> argument must be an integer greater than 0.
	<b>time</b> <i>interval</i>	(Optional) Specifies the time interval during which the one or more occurrences must take place. When the keyword is not specified, no time period check is applied.  The <i>interval</i> argument is an integer that represents seconds in the range from 0 to 4294967295.

**Defaults** None

**Command Modes** Applet configuration (config-applet)

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	5.2.(1)	Added the <b>tag</b> <i>tag</i> keywords.
	4.0(1)	This command was introduced.

**Usage Guidelines** The **event cli match** *regex* command must meet the following criteria:

1. It must be a fully qualified CLI string that must include the complete, not relative, path. For example, to describe the **shutdown** command under interface mode, the command should be:

```
switch(config-applet)# event cli match "conf t ; interface * ; shutdown"
```



2. The delimiter between the modes must be “;”, which is a space followed by a semi-colon and followed by another space.

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 "write memory.*" time 13
switch(config-applet)#
```

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

```
no event counter name name
```

Syntax Description	
<b>tag</b> <i>tag</i>	(Optional) Identifies this specific event when multiple events are included in the policy.
<b>name</b> <i>name</i>	Specifies the name of the counter that will be monitored. The <i>name</i> identifier can be any string value.
<b>entry-val</b> <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 —2147483648 to 2147483647, inclusive.
<b>entry-op</b> <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"> <li>• <b>gt</b>—Greater than</li> <li>• <b>ge</b>—Greater than or equal to</li> <li>• <b>eq</b>—Equal to</li> <li>• <b>ne</b>—Not equal to</li> <li>• <b>lt</b>—Less than</li> <li>• <b>le</b>—Less than or equal to</li> </ul> <p>If there is a match, an event is triggered and event monitoring is disabled until the exit criteria are met.</p>
<b>exit-val</b> <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 —2147483648 to 2147483647, inclusive.
<b>exit-op</b> <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"> <li>• <b>gt</b>—Greater than</li> <li>• <b>ge</b>—Greater than or equal to</li> <li>• <b>eq</b>—Equal to</li> <li>• <b>ne</b>—Not equal to</li> <li>• <b>lt</b>—Less than</li> <li>• <b>le</b>—Less than or equal to</li> </ul> <p>If there is a match, an event is triggered and event monitoring is reenabled.</p>

### Defaults

None

---

**Command Modes** Applet configuration (config-applet)

---

**SupportedUserRoles** network-admin  
vdc-admin

---

Command History	Release	Modification
	5.2.(1)	Added the <b>tag</b> <i>tag</i> keywords.
	4.0(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)#
```

# 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

<b>fan number</b>	(Optional) Specifies a fan number to monitor for a fan absent event. The range is from 1 to 4.
<b>time interval</b>	Specifies the time interval (in seconds) within which the fan can stay absent. The range is from 0 to 4294967295.

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(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 42
switch(config-applet)#
```

# 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	
<b>fan number</b>	(Optional) Specifies a fan number to monitor for a fan bad event. The range is from 1 to 4.
<b>time interval</b>	Specifies the time interval (in seconds) within which the fan can stay bad. The range is from 0 to 4294967295.

**Defaults** None

**Command Modes** Applet configuration (config-applet)

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(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 42
switch(config-applet)#
```

# event gold

To specify an event criteria for an Embedded Event Manager (EEM) applet that is run on the basis of a Generic Online Diagnostic (GOLD) failure event when monitoring one or more modules, use the **event gold** command. To remove the GOLD failure event criteria, use the **no** form of this command.

```
event gold [failure-type {sup | fabric | lc | port}] module {module | all} test { name | test-id }
    [severity {minor | moderate | major}] testing-type {bootup | ondemand | scheduled |
monitoring} consecutive-failure cnt
```

```
no event gold [failure-type {sup | fabric | lc | port}] module {module | all} test { name | test-id }
```

## Syntax Description

<b>failure-type</b>	Specifies the GOLD failure event type: <ul style="list-style-type: none"> <li><b>sup</b>—Specifies the supervisor failure event (default action is switchover).</li> <li><b>fabric</b>—Specifies the fabric card failure event (default action is fabric reload or poweroff).</li> <li><b>lc</b>—Specifies the linecard failure event (default action is module reload or poweroff).</li> <li><b>port</b>—Specifies the port failure event (default action is port error disable).</li> </ul>
<b>module</b>	Specifies that one module or all modules must be monitored: <p><b>Note</b> The <b>module</b> keyword is required to complete the <b>event gold</b> command.</p>
<i>module</i>	Number of a specific module to be monitored.
<b>all</b>	Specifies that all modules are to be monitored.
<b>test name</b>	Specifies the test name of the event criteria. The range is
<i>test-id</i>	Specifies the test ID of the event criteria. The test ID is in the range of 1 to 30.
<b>severity</b>	(Optional) Specifies the event criteria match for the diagnostic result matches with the GOLD diagnostic error: <ul style="list-style-type: none"> <li><b>minor</b>—Specifies to match to minor GOLD diagnostic errors.</li> <li><b>moderate</b>—Specifies to match moderate GOLD diagnostic errors.</li> <li><b>major</b>—Specifies to match major GOLD diagnostic errors.</li> </ul>
<b>testing-type</b>	Specifies the event criteria based on the testing types of diagnostic from GOLD: <ul style="list-style-type: none"> <li><b>bootup</b>—Specifies the diagnostic tests running on system bootup.</li> <li><b>ondemand</b>—Specifies the diagnostic tests running from CLI after the module is online.</li> <li><b>schedule</b>—Specifies the scheduled diagnostic tests.</li> <li><b>monitoring</b>—Specifies the diagnostic tests that are running periodically in the background to monitor the health of the system.</li> </ul>
<b>consecutive-failure</b> <i>cnt</i>	Specifies the event criteria based on consecutive test failure information from GOLD.

## Defaults

None

---

**Command Modes** Applet configuration (config-applet)

---

**SupportedUserRoles** network-admin  
vdc-admin

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(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 new GOLD failure event occurs for any module:

```
switch# configure terminal  
switch(config)# event manager applet gold-match  
switch(config-applet)# event gold module all test atBoot testing-type bootup  
switch(config-applet)#
```

# event manager applet

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

**event manager applet** *applet-name* [**override** *policy-name*] [**class** *class-options*]

**no event manager applet** *applet-name*

## Syntax Description

<i>applet-name</i>	Unique identifier for the applet. This identifier can be any string value.
<b>override</b> <i>policy-name</i>	(Optional) Specifies this policy will override a system policy. <i>policy-name</i> is the name of the system policy to override. It should begin with a double underscore.
<b>class</b> <i>class-options</i>	(Optional) Specifies the EEM policy class. <i>class-options</i> can be either one of the following: <ul style="list-style-type: none"> <li><i>class-letter</i>: Letter from A to Z that identifies each policy class. Specify any one class-letter.</li> <li><b>default</b>: Policies registered with the default class.</li> </ul>

## Defaults

None

## Command Modes

Global configuration

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.
7.2(0)D1(1)	This command was modified to add class options

## Usage Guidelines

This command does not require a license.

## Examples

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

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



# event manager clear counter

To specify an Embedded Event Manager (EEM) counter to clear, use the **event manager clear counter** command.

**event manager clear counter** *counter-name*

<b>Syntax Description</b>	<i>counter-name</i> Name of the counter to clear.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Applet configuration (config-applet)
----------------------	--------------------------------------

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to clear an EEM counter:
-----------------	---

```
switch# configure terminal
switch(config)# event manager clear counter eem-counter
switch(config)#
```

# event manager clear history events

To clear all Embedded Event Manager (EEM) event history, use the **event manager clear history events** command.

## event manager clear history events

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

**Defaults** None

**Command Modes** Applet configuration (config-applet)

**SupportedUserRoles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to clear all of the EEM event history:

```
switch# configure terminal
switch(config)# event manager clear history events
switch(config)#
```

# event manager environment

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

**event manager environment** *varname varvalue*

**no event manager environment** *varname*

Syntax	Description
<i>varname</i>	Name of the EEM environment variable.
<i>varvalue</i>	String of characters, including embedded spaces, to be placed in the environment variable <i>varname</i> .

**Defaults** None

**Command Modes** Embedded event manager

**Supported User Roles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to set an EEM environment variable:

```
switch# configure terminal
switch(config)# event manager environment _cron_entry 0-59/2 0-23/1 * * 0-7
switch(config)#
```

# event manager policy

To register an Embedded Event Manager (EEM) policy with the EEM, use the **event manager policy** command. To remove the event manager policy command from the configuration file, use the **no** form of this command.

**event manager policy** *VSHscriptfilename*

**no event manager policy** *VSHscriptfilename*

## Syntax Description

*VSHscriptfilename* Name of the VSH script file to register with the EEM. This name becomes the name of the EEM policy.

**Note** System policy names begin with two underscore characters (\_\_).

## Defaults

None

## Command Modes

Applet configuration (config-applet)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

The EEM schedules and runs policies on the basis of an event specification that is contained within the policy itself. When the **event manager policy** command is invoked, the EEM examines the policy and registers it to be run when the specified event occurs.

## Examples

This example shows how to register a policy:

```
switch# configure terminal
switch(config)# event manager policy fanpolicy.vsh
switch(config)#
```

# event manager run

To manually run a registered Embedded Event Manager (EEM) policy, use the **event manager run** command.

**event manager run** *policy-name*

<b>Syntax Description</b>	<i>policy-name</i>	Name of the registered EEM policy to run.
	<b>Note</b>	System policy names begin with two underscore characters (__).

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Applet configuration (config-applet)
----------------------	--------------------------------------

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to manually run a registered EEM policy:

```
switch# configure terminal
switch(config)# event manager run fanpolicy.vsh
switch(config)#
```

# event manager scheduler

To schedule Embedded Event Manager (EEM) policies and set the policy scheduling options, use the **event manager scheduler** command in global configuration mode. To remove the scheduling of EEM policies, use the **no** form of this command.

**event manager scheduler applet thread class** *class-options* **number** *thread-number*

**no event manager scheduler applet thread class** *class-options* **number** *thread-number*

## Syntax Description

<b>applet</b>	Specifies the EEM applet policy
<b>thread</b>	Specifies the thread for the class
<b>class</b> <i>class-options</i>	Specifies the EEM policy class.  <i>class-options</i> can be one or a combination of the following: <ul style="list-style-type: none"> <li><i>class-letter</i>: Letter from A to Z that identifies each policy class. You can specify multiple instances of <i>class-letter</i>.</li> <li><b>default</b>: Specifies policy registered with default class.</li> <li><b>range</b> <i>class-letter-range</i>: Specifies a range of EEM policy class. Multiple instances of <b>range</b> <i>class-letter-range</i> can be specified. The letters used in <i>class-letter-range</i> must be in uppercase.</li> </ul>
<b>number</b> <i>thread-number</i>	Specifies the number of concurrent execution threads for the specified class.  <i>thread-number</i> is in the range of 1 to 65535.

## Defaults

Policy scheduling is active.

## Command Modes

Global Configuration (config#).

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

During registration, EEM policies will be assigned a class if **class** *class-letter* is specified by the **event manager applet** or **event manager policy** commands. EEM policies registered without a class will be assigned the **default** class. Threads that have **default** as the class will service the default class when the thread is available for work. Threads that are assigned specific class letters will service any policy with a matching class letter.

If there is no EEM execution thread available to run the policy in the specified class and a scheduler rule for the class is configured, the policy will wait until a thread of that class is available for execution. Synchronous policies that are triggered from the same input event should be scheduled in the same execution thread.

For **class**, specify any of these options- *class-letter*, **default**, or **range** *class-letter-range*. You can specify all these options in the same CLI statement.

To schedule EEM policies and set the script scheduling options, use the **event manager scheduler script** command in global configuration mode. To remove the EEM script scheduling options and restore the default value, use the **no** form of this command.

### Examples

The following example shows how to create two EEM scheduling threads to run applets of the default class:

```
switch# configure terminal
switch(config)# event manager scheduler applet thread class default number 2
```

The following example shows how to create one EEM execution thread to run Tcl scripts of class A, B, D and E.

```
switch(config)# event manager scheduler script thread class A B range D-E number 1
```

### Related Commands

Command	Description
<b>event manager applet</b>	Registers an EEM applet with the EEM and enters applet configuration mode.
<b>event manager policy</b>	Registers an EEM policy with the EEM.
<b>event manager scheduler hold</b>	Holds the EEM policy scheduling execution.
<b>event manager scheduler script</b>	Sets the options for EEM script scheduling.
<b>debug event manager scheduler suspend</b>	Suspends the EEM policy scheduling execution.

# event manager scheduler clear

To clear Embedded Event Manager (EEM) policies that are executing or pending execution, use the **event manager scheduler clear** command in privileged EXEC mode.

```
event manager scheduler clear {all | policy job-id | queue-type applet [class class-options]}
[processor {rp_primary | rp_standby}]
```

## Syntax Description

<b>all</b>	Clears all policies that are currently executing or pending execution.
<b>policy job-id</b>	Clears the EEM policy specified by the <i>job-id</i> . <i>job-id</i> is a number in the range of 1 to 4294967295 that identifies each policy in the queue.
<b>queue-type</b>	Clears the queue type of the EEM policy.
<b>applet</b>	Specifies the EEM queue type, applet.
<b>class class-options</b>	(Optional) Clears the EEM policies of a specified class. <i>class-options</i> can be one or a combination of the following: <ul style="list-style-type: none"> <li><b>class-letter</b>: Letter from A to Z that identifies each policy class. You can specify multiple instances of <i>class-letter</i>.</li> <li><b>default</b>: Specifies policy registered with default class.</li> <li><b>range class-letter-range</b>: Specifies a range of EEM policy class. Multiple instances of <b>range class-letter-range</b> can be specified. The letters used in <i>class-letter-range</i> must be in uppercase.</li> </ul>
<b>processor</b>	(Optional) Specifies the processor to execute the command.
<b>rp_primary</b>	(Optional) Indicates the default Route Processor (RP). The policy runs on the primary RP when an event correlation causes the policy to be scheduled.
<b>rp_standby</b>	(Optional) Indicates the standby RP. The policy runs on the standby RP when an event correlation causes the policy to be scheduled.

## Defaults

None.

## Command Modes

Privileged EXEC.

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

For **class**, specify at least one of the options: *class-letter*, **default**, or **range class-letter-range**. You can specify all these options in the same CLI statement.



**Examples**

The following example shows how to clear EEM policies that are pending execution. The show commands display sample output before and after the policy is cleared.

```
switch# show event manager policy pending
no. job id status time of event          event type      name
1   1      pend  Thu Sep 7  02:54:04 2006  syslog         applet: one
2   2      pend  Thu Sep 7  02:54:04 2006  syslog         applet: two
3   3      pend  Thu Sep 7  02:54:04 2006  syslog         applet: three

switch# event manager scheduler clear policy 2
switch# show event manager policy pending
no. job id status time of event          event type      name
1   1      pend  Thu Sep 7  02:54:04 2006  syslog         applet: one
3   3      pend  Thu Sep 7  02:54:04 2006  syslog         applet: three
```

**Related Commands**

Command	Description
<b>event manager policy</b>	Registers an EEM policy with the EEM.
<b>show event manager policy pending</b>	Displays EEM policies that are pending execution.

# event manager scheduler hold

To hold a scheduled Embedded Event Manager (EEM) policy event or event queue in the EEM scheduler, use the **event manager scheduler hold** command in the privileged EXEC mode. To resume the policy event or event queue, use the **event manager scheduler release** command.

**event manager scheduler hold** {**all** | **policy** *job-id* | **queue-type** **applet** [**class** *class-options*]}

## Syntax Description

<b>all</b>	Holds all the EEM policy event or event queue in the EEM scheduler.
<b>policy</b> <i>job-id</i>	Holds the EEM policy event or event queue in the EEM scheduler as specified by the <i>job-id</i> .  <i>job-id</i> is a number in the range of 1 to 4294967295 that identifies each policy in the queue.
<b>queue-type</b>	Holds the EEM policy event or event based on the EEM queue type.
<b>applet</b>	Specifies the EEM queue type, applet.
<b>class</b> <i>class-options</i>	(Optional) Specifies the EEM policy class.  <i>class-options</i> can be one or all of the following: <ul style="list-style-type: none"> <li><b>class-letter</b> : Letter from A to Z that identifies each policy class. You can specify multiple instances of <i>class-letter</i>.</li> <li><b>default</b>: Specifies the policy registered with default class.</li> <li><b>range</b> <i>class-letter-range</i>: Specifies a range of EEM policy class. Multiple instances of <b>range</b> <i>class-letter-range</i> can be specified. The letters used in <i>class-letter-range</i> must be in uppercase.</li> </ul>

## Defaults

None.

## Command Modes

Privileged EXEC.

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

Use the **show event manager policy pending** command to display the policies pending in the server execution queue.

Use the **event manager scheduler hold** command to hold a policy or a policy queue in the server.

For **class**, specify any of the options- *class-letter*, **default**, and **range** *class-letter-range*. You can specify all these options in the same CLI statement.

**Examples**

The following example shows how to hold a scheduled policy event in the EEM scheduler. The **show** commands display sample output before and after the policy event is held.

```
switch# show event manager policy pending
no. job id status time of event          event type    name
1  1      pend  Thu Sep 7 02:54:04 2006  syslog       applet: one
2  2      pend  Thu Sep 7 02:54:04 2006  syslog       applet: two
3  3      pend  Thu Sep 7 02:54:04 2006  syslog       applet: three
switch# event manager scheduler hold policy 2
switch# show event manager policy pending
no. job id status time of event          event type    name
1  1      pend  Thu Sep 7 02:54:04 2006  syslog       applet: one
2  2      held  Thu Sep 7 02:54:04 2006  syslog       applet: two
3  3      pend  Thu Sep 7 02:54:04 2006  syslog       applet: three
```

**Related Commands**

Command	Description
<b>event manager policy</b>	Registers an EEM policy with the EEM.
<b>event manager scheduler release</b>	Resumes the policy event or event queue.
<b>show event manager policy pending</b>	Displays EEM policies that are pending execution.

# event manager scheduler modify

To modify the scheduling parameters of the Embedded Event Manager (EEM) policies, use the **event manager scheduler modify** command in the privileged EXEC mode.

```
event manager scheduler modify {all | policy job-id | queue-type applet} {class class-options
[queue-priority { high | last | low | normal}] | queue-priority { high | last | low | normal} [class
class-options]}
```

Syntax Description		
<b>all</b>	Changes all EEM policies that are currently executing or in the pending execution mode.	
<b>policy <i>job-id</i></b>	Changes the EEM policy specified by the <i>job-id</i> . <i>job-id</i> is a number in the range of 1 to 4294967295 that identifies each policy in the queue.	
<b>queue-type</b>	Changes the queue type of EEM policy.	
<b>applet</b>	Specifies the EEM queue type, applet.	
<b>class <i>class-options</i></b>	Specifies the EEM policy class. <i>class-options</i> can be one or all of the following: <ul style="list-style-type: none"> <li><b>class-letter:</b> Letter from A to Z that identifies each policy class. You can specify multiple instances of <i>class-letter</i>.</li> <li><b>default:</b> Specifies policy registered with default class.</li> </ul>	
<b>queue-priority</b>	(Optional) Changes the priority of the queuing order of the EEM policies.	
<b>high</b>	(Optional) Specifies the queue priority as high.	
<b>last</b>	(Optional) Specifies the queue priority as last.	
<b>low</b>	(Optional) Specifies the queue priority as low.	
<b>normal</b>	(Optional) Specifies the queue priority as normal.	

**Defaults** None.

**Command Modes** Privileged EXEC.

Command History	Release	Modification
	7.2(0)D1(1)	This command was introduced.

**Usage Guidelines** Use the **show event manager policy pending** command to display the policies pending in the server execution queue.

Use the **event manager scheduler modify** command to modify the scheduling parameters of a policy.

For **class**, specify any of the options- *class-letter* or **default**. You can specify all these options in the same CLI statement..

### Examples

The following example shows how to modify the scheduling parameters of EEM policies. The **show** commands display sample output before and after the scheduling parameters are modified.

```
switch# show event manager policy pending
no. job id status time of event          event type      name
1  default pend   Thu Sep 7 02:54:04 2006  syslog         applet: one
2  default pend   Thu Sep 7 02:54:04 2006  syslog         applet: two
3  B          pend   Thu Sep 7 02:54:04 2006  syslog         applet: three
switch# event manager scheduler modify all class A
switch# show event manager policy pending
no. job id status time of event          event type      name
1  A          pend   Thu Sep 7 02:54:04 2006  syslog         applet: one
2  A          pend   Thu Sep 7 02:54:04 2006  syslog         applet: two
3  A          pend   Thu Sep 7 02:54:04 2006  syslog         applet: three
```

### Related Commands

Command	Description
<b>event manager policy</b>	Registers an EEM policy with the EEM.
<b>show event manager policy pending</b>	Displays EEM policies that are pending execution.

# event manager scheduler release

To resume execution of the specified Embedded Event Manager (EEM) policies, use the **event manager scheduler release** command in the privileged EXEC mode.

**event manager scheduler release** {**all** | **policy** *job-id* | **queue-type** **applet** [**class** *class-options*]}

## Syntax Description

<b>all</b>	Resumes execution of all EEM policies.
<b>policy</b> <i>job-id</i>	Resumes the EEM policy specified by the <i>job-id</i> . <i>job-id</i> is a number in the range of 1 to 4294967295 that identifies each policy in the queue.
<b>queue-type</b>	Resumes execution of policies based on EEM queue type.
<b>applet</b>	Specifies the EEM applet.
<b>class</b> <i>class-options</i>	Specifies the EEM policy class. <i>class-options</i> can be one or all of the following: <ul style="list-style-type: none"> <li><i>class-letter</i>: Letter from A to Z that identifies each policy class. You can specify multiple instances of <i>class-letter</i>.</li> <li><b>default</b>: Specifies the policy registered with default class.</li> <li><b>range</b> <i>class-letter-range</i>: Specifies a range of EEM policy class. Multiple instances of <b>range</b> <i>class-letter-range</i> can be specified. The letters used in <i>class-letter-range</i> must be in uppercase.</li> </ul>

## Defaults

By default the command is disabled.

## Command Modes

Privileged EXEC.

## Command History

Release	Modification
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

To release the EEM policies held using the **event manager scheduler hold** command, use the **event manager scheduler release** command.

For **class**, specify any of the options: *class-letter*; **default** or **range** *class-letter-range*. You can specify all these options in the same CLI statement.

## Examples

The following example shows how to resume the execution of all EEM policies.

```
switch# show event manager release all
```

The following example shows how to resume the execution for policies of class A to E.

```
switch# event manager scheduler release queue-type applet class range A-E
```

Related Commands	Command	Description
	event manager scheduler hold	Holds the policy event or event queue.

## event module-failure

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

```
event module-failure type err-name module {all | module} count count [time interval]
```

```
no event module-failure type err-name module {all | module} count count
```

### Syntax Description

<b>type</b> <i>err-name</i>	Specifies the type of failure condition. Select one of the <i>err-name</i> conditions: <b>any</b> —Any failure <b>addon-sequence-failure</b> —Addon sequence failure <b>hitless-upgrade-diag-failure</b> —Runtime diagnostic failure after hitless upgrade <b>hitless-upgrade-failure</b> —Hitless upgrade failure <b>hitless-upgrade-procmgr-notif</b> —LC software failure after hitless upgrade <b>hitless-upgrade-reg-failure</b> —Registration failure after hitless upgrade <b>hitless-upgrade-seq-timeout</b> —Hitless upgrade sequence timeout <b>image-download-failed</b> —Image download failure <b>image-upgrade-failed</b> —Image upgrade failed <b>insertion-seq-failure</b> —Insertion sequence failure <b>lc-failed</b> —LC failed <b>lc-not-responding</b> —LC not responding <b>lc-ready-timeout</b> —LC ready timeout <b>lc-sw-failure</b> —LC software failure <b>registration-failure</b> —Registration failure <b>registration-timeout</b> —Registration timeout <b>runtime-diag-failure</b> —Runtime diag failure <b>runtime-diag-timeout</b> —Runtime diag timeout <b>sequence-timeout</b> —Sequence timeout <b>srg-info-resp-timeout</b> —SRG info response timeout <b>unexpected-registration</b> —Unexpected registration received <b>upgrade-srg-not-compatible</b> —Upgrade SRG not compatible
<b>module</b>	Specifies that one module or all modules must be monitored.
<i>module</i>	Number of a specific module to be monitored.
<b>all</b>	Specifies that all modules are to be monitored.
<b>count</b> <i>count</i>	Specifies the number of matching occurrences before a module failure event is triggered. The range is from 0 to 4294967295.
<b>time</b> <i>interval</i>	(Optional) Specifies the time interval (in seconds) within which the events need to happen. The range is from 0 to 4294967295.



---

**Defaults** None

---

**Command Modes** Embedded event manager

---

**SupportedUserRoles** network-admin  
vdc-admin

---

Command History	Release	Modification
	5.2.(1)	Added the <b>tag tag</b> keywords.
	4.0(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 module failure event occurs:

```
switch# configure terminal
switch(config)# event manager applet modfail-applet
switch(config-applet)# event module-failure type unexpected-registration module 6 count 2
switch(config-applet)#
```

# event module status

To configure a status event on a module, use the **event module status** command. To remove the status event configuration, use the **no** form of this command.

```
event module status {online | offline | any} module {all | module-number}
```

```
no event module status {online | offline | any} module {all | module-number}
```

## Syntax Description

<b>online</b>	Specifies the online status.
<b>offline</b>	Specifies the offline status.
<b>any</b>	Specifies the online or offline status.
<b>module</b>	Specifies a module.
<b>all</b>	Specifies all modules.
<i>module-number</i>	Module number. The range is from 1 to 18.

## Defaults

None

## Command Modes

Applet Configuration (config-applet)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure a status event on a module:

```
switch(config)# event manager applet EVM1  
switch(config-applet)# event module status any module 10  
switch(config-applet)#
```

This example shows how to remove the status event configuration:

```
switch(config-applet)# no event module status any module 10  
switch(config-applet)#
```

Related Commands	Command	Description
	<b>event manager applet</b>	Registers an applet with the Embedded Event Manager (EEM).
	<b>event manager policy</b>	Registers an Embedded Event Manager (EEM) policy with the EEM.

# event oir

To specify that an Embedded Event Manager (EEM) applet be run on the basis of an event raised when a hardware online insertion and removal (OIR) occurs, use the **event oir** command. This command has three forms; **fan**, **module**, and **powersupply**. To remove the OIR specification from the configuration, use the **no** form of this command.

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

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

Syntax Description	
<b>tag tag</b>	(Optional) Identifies this specific event when multiple events are included in the policy.
<b>fan</b>	Specifies the system fans. Optionally, specify an individual fan.
<b>module</b>	Specifies the system modules. Optionally, specify an individual module.
<b>powersupply</b>	Specifies the system power supplies. Optionally, specify an individual power supply.
<b>insert</b>	Specifies to insert OIR.
<b>remove</b>	Specifies to remove OIR.
<b>anyoir</b>	Specifies to either insert or remove OIR.
<i>number</i>	(Optional) If you selected <b>fan</b> , enter a fan number to monitor for an OIR event. The range is from 1 to 4. If you selected <b>module</b> , enter a module number to monitor for an OIR event. The range is from 1 to 10. If you selected <b>powersupply</b> , enter a power supply number to monitor for an OIR event. The range is from 1 to 3.

**Defaults** None

**Command Modes** Applet Configuration (config-applet)

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	5.2.(1)	Added the <b>tag tag</b> keywords.
	4.0(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 be run on the basis of an event raised when a module OIR occurs:

```
switch# configure terminal
switch(config)# event manager applet oir-applet
switch(config-applet)# event oir module anyoir
switch(config-applet)#
```

# event policy-default

To use the event if 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 interval**]

**no event policy-default count** *count*

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

**Defaults** None

**Command Modes** Applet Configuration (config-applet)

**SupportedUserRoles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to use the event in the system policy being overridden:

```
switch# configure terminal
switch(config)# event policy-default count 6
switch(config)#
```

## 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 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

<b>tag</b> <i>tag</i>	(Optional) Identifies this specific event when multiple events are included in the policy.
<b>oid</b> <i>value</i>	Specifies the SNMP object identifier (object ID) 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 <b>oid</b> keyword is used, an error message is returned if the OID is not one of the following: <ul style="list-style-type: none"> <li>• INTEGER_TYPE</li> <li>• COUNTER_TYPE</li> <li>• GAUGE_TYPE</li> <li>• TIME_TICKS_TYPE</li> <li>• COUNTER_64_TYPE</li> <li>• OCTET_PRIM_TYPE</li> <li>• OPAQUE_PRIM_TYPE</li> </ul>
<b>get-type</b>	Specifies the type of SNMP get operation to be applied to the object ID specified by the <b>oid</b> <i>value</i> argument.
<b>exact</b>	Retrieves the object ID specified by the <b>oid</b> <i>value</i> argument.
<b>next</b>	Retrieves the object ID that is the alphanumeric successor to the object ID specified by the <b>oid</b> <i>value</i> argument.
<b>entry-op</b> <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"> <li>• <b>gt</b>—Greater than</li> <li>• <b>ge</b>—Greater than or equal to</li> <li>• <b>eq</b>—Equal to</li> <li>• <b>ne</b>—Not equal to</li> <li>• <b>lt</b>—Less than</li> <li>• <b>le</b>—Less than or equal to</li> </ul> <p>If there is a match, an event is triggered and event monitoring is disabled until the exit criteria are met.</p>

<b>entry-val</b> <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.
<b>exit-comb</b>	(Optional) Indicates the combination of exit conditions that must be met before event monitoring is reenabled.
<b>or</b>	(Optional) Specifies that an exit comparison operator and an exit object ID value or an exit time value must exist.
<b>and</b>	(Optional) Specifies that an exit comparison operator, an exit object ID value, and an exit time value must exist.
<b>exit-op</b> <i>op</i>	(Optional) Compares the contents of the current object ID with the exit value using the specified operator: <ul style="list-style-type: none"> <li>• <b>gt</b>—Greater than</li> <li>• <b>ge</b>—Greater than or equal to</li> <li>• <b>eq</b>—Equal to</li> <li>• <b>ne</b>—Not equal to</li> <li>• <b>lt</b>—Less than</li> <li>• <b>le</b>—Less than or equal to</li> </ul> <p>If there is a match, an event is triggered and event monitoring is reenabled.</p> <p><b>Note</b> This keyword and its argument are not optional if the <b>exit-comb</b> keyword is defined.</p>
<b>exit-val</b> <i>value</i>	(Optional) Specifies the value with which the contents of the current object ID are compared to decide whether the exit criteria are met. <p><b>Note</b> This keyword and its argument are not optional if the <b>exit-comb</b> keyword is defined.</p>
<b>poll-interval</b> <i>value</i>	Specifies the time interval between consecutive polls. The <i>value</i> argument is an integer that represents seconds in the range from 1 to 4294967295. The minimum polling interval is 1 second.

**Defaults**

None

**Command Modes**

Applet Configuration (config-applet)

**Supported User Roles**network-admin  
vdc-admin**Command History**

Release	Modification
5.2.(1)	Added the <b>tag tag</b> keywords.
4.0(1)	This command was introduced.

**Usage Guidelines**

This command does not require a license.



---

**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 2
switch(config-applet)#
```

# 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 event, 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** Applet Configuration (config-applet)

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(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 event occurs:

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

# event syslog

To configure Cisco NX-OS Embedded Event Manager (EEM) to monitor an event, use the **event syslog** command. To remove the syslog configuration, use the **no** form of this command.

**event syslog** [ **tag** *tag*] [**occurs** | **pattern** *msg-text* | **period** | **priority** [0-7 | **emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **informational** | **debugging**]]

**no event syslog** [**tag** *tag*] [**occurs** | **pattern** *msg-text* | **period** | **priority** [0-7 | **emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **informational** | **debugging**]]

Syntax Description	
<b>tag</b> <i>tag</i>	(Optional) Identifies this specific event when multiple events are included in the policy.
<b>occurs</b>	(Optional) Specifies the number of occurrences. The range is from 1 to 65000.
<b>pattern</b> <i>msg-text</i>	(Optional) Specifies the matching regular expression (regex). The pattern can contain character text, an environment variable, or a combination of the two. If the string contains embedded blanks, it is enclosed with double quotation marks.
<b>period</b>	(Optional) Specifies the time interval during which the event occurs. The range is from 0 to 4294967295.
<b>priority</b>	(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.
<b>0-7</b>	(Optional) Enters the priority of the log message.
<b>emergencies</b>	(Optional) Specifies that the system is unusable.
<b>alerts</b>	(Optional) Specifies that immediate action is needed.
<b>critical</b>	(Optional) Specifies critical conditions.
<b>errors</b>	(Optional) Specifies error conditions.
<b>warnings</b>	(Optional) Specifies warning conditions.
<b>notifications</b>	(Optional) Specifies normal but significant conditions.
<b>informational</b>	(Optional) Specifies informational messages. This is the default.
<b>debugging</b>	(Optional) Specifies debugging messages.

**Defaults** None

**Command Modes** Embedded event manager

**SupportedUserRoles** network-admin  
vdc-admin

**Command History**

Release	Modification
5.2(1)	Added the <b>tag</b> <i>tag</i> keywords.
5.1(1)	This command was introduced.

**Usage Guidelines**

This command does not require a license.

**Examples**

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

```
switch# configure terminal
switch(config-applet)# event syslog occurs 10 pattern "authentication failed"
Configuration accepted successfully
```

This example shows how to remove the syslog message monitor configuration:

```
switch# configure terminal
switch(config-applet)# event syslog occurs 10 pattern "authentication failed"
Configuration accepted successfully
```

**Related Commands**

Command	Description
<b>action syslog</b>	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

# 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** form of this command.

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

```
no event temperature threshold {major | minor | any}
```

## Syntax Description

<b>module</b> <i>module</i>	(Optional) Specifies that a specific module must be monitored. The range is from 1 to 10.
<b>sensor</b> <i>number</i>	(Optional) Specify that a specific <b>sensor</b> must be monitored. The range is from 1 to 18.
<b>threshold</b>	Specifies the threshold event that triggers the EEM applet. Choose either <b>major</b> , <b>minor</b> , or <b>any</b> (major or minor).
<b>major</b>	Specifies a major event.
<b>minor</b>	Specifies a minor event.
<b>any</b>	Specifies any event.

## Defaults

None

## Command Modes

Applet Configuration (config-applet)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(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)#
```

# 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		
<b>tag</b> <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.	
<b>state</b>	Specifies that the tracked object transition causes an event to be raised.	
<b>up</b>	Specifies an event is to be raised when the tracked object transitions from a down state to an up state.	
<b>down</b>	Specifies an event is to be raised when the tracked object transitions from an up state to a down state.	
<b>any</b>	Specifies an event is to be raised when the tracked object transitions to or from any state.	

**Defaults** None

**Command Modes** Applet Configuration (config-applet)

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	5.2.(1)	Added the <b>tag</b> <i>tag</i> keywords.
	4.0(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 42 state down
switch(config-applet)#
```



# exporter

To specify a NetFlow exporter to use for a NetFlow monitor, use the **exporter** command. To remove a NetFlow exporter, use the **no** form of this command.

**exporter** *name*

**no exporter** *name*

## Syntax Description

<i>name</i>	Name of the exporter.
-------------	-----------------------

## Defaults

None

## Command Modes

NetFlow monitor configuration (config-flow-monitor)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure a NetFlow exporter for a NetFlow monitor:

```
switch(config)# flow monitor Custom-Flow-Monitor-1
switch(config-flow-monitor)# exporter Custom-Flow-Exporter-1
switch(config-flow-monitor)#
```

This example shows how to remove a NetFlow exporter:

```
switch(config-flow-monitor)# no exporter
```

## Related Commands

Command	Description
<b>show flow sw-monitor</b>	Displays information about NetFlow monitors.





# F Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter F.

# feature icam

To enable the Intelligent CAM (iCAM) feature, use the **feature icam** command. To disable the iCAM feature, use the **no** form of this command.

**feature icam**

**no feature icam**

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

**Command Default** The iCAM feature is not enabled.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco NX-OS Release 8.0(1)	This command was introduced.

**Usage Guidelines** This feature requires the ENHANCED\_LAYER2\_PKG license.

**Examples** This example shows how to enable the iCAM feature:

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

This example shows how to disable the iCAM feature:

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

Related Commands	Command	Description
	<b>icam monitor entries</b>	Enables monitoring on the TCAM entries.
	<b>icam monitor interval</b>	Configures the iCAM monitor interval and the number of intervals in an iCAM monitor history.
	<b>icam monitor resource</b>	Enables iCAM monitoring on TCAM resources.
	<b>show icam entries acl</b>	Displays traffic analytics of the ACL TCAM, which includes RACL, VACL, QoS, PBR, WCCP, CoPP, and so on.
	<b>show icam entries multicast</b>	Displays traffic analytics of multicast entries.

<b>Command</b>	<b>Description</b>
<b>show icam prediction entries acl</b>	Displays machine-learning predictive analytics of TCAM entries.
<b>show icam prediction entries multicast</b>	Displays machine-learning predictive analytics of multicast entries.
<b>show icam prediction resource</b>	Displays machine-learning predictive analytics of TCAM resource utilization.
<b>show icam resource</b>	Displays TCAM resource utilization.

# feature lldp

To enable the Link Layer Discovery Protocol (LLDP) feature globally, use the **feature lldp** command. To disable the LLDP feature, use the **no** form of this command.

**feature lldp**

**no feature lldp**

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

**Defaults** Disabled

**Command Modes** Global configuration mode (config)

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** In order for LLDP to discover servers connected to your device, the servers must be running openLLDP software.

LLDP must be enabled on the device before you can enable or disable it on any interfaces.



**Note**

LLDP is supported only on physical interfaces. LLDP timers and type, length, and value (TLV) descriptions cannot be configured using Cisco DCNM.

LLDP can discover up to one device per port. LLDP can discover up to one server per port. LLDP can discover only Linux servers that are connected to your device. LLDP can discover Linux servers, if they are not using a converged network adapter (CNA); however, LLDP cannot discover other types of servers.

Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the **switchto vdc** command.

This command does not require a license.

**Examples** This example shows how to enable the LLDP feature globally:

```
switch(config)# feature lldp  
switch(config)
```

This example shows how to disable the LLDP feature:

```
switch(config)# no feature lldp  
switch(config)#2010 Jan 11 01:50:33 switch %FEATURE-MGR-2-FM_AUTOCKPT_IN_PROGRESS:  
AutoCheckpoint system-fm-lldp's creation in progress...  
2010 Jan 21 01:50:34 switch %FEATURE-MGR-2-FM_AUTOCKPT_SUCCEEDED: AutoCheckpoint  
created successfully  
switch(config)#
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show running-config lldp</b>	Displays the global LLDP configuration.

---

# feature netflow

To globally enable the NetFlow feature, use the **feature netflow** command. To disable NetFlow, use the **no** form of this command.

**feature netflow**

**no feature netflow**

**Syntax Description** This command does not have any arguments or keywords.

**Defaults** Disabled

**Command Modes** Global configuration mode

**SupportedUserRoles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to enable NetFlow on a Cisco NX-OS device:

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

This example shows how to disable NetFlow on a Cisco NX-OS device:

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

Related Commands	Command	Description
	<b>flow record</b>	Creates a flow record and enters flow record configuration mode.
	<b>show flow record</b>	Displays information about NetFlow flow records.

# feature ntp

To enable the Network Time Protocol (NTP) on a virtual device context (VDC), use the **feature ntp** command. To disable NTP on a VDC, 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

**SupportedUserRoles** network-admin  
vdc-admin

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

**Usage Guidelines** Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.

This command does not require a license.

**Examples** This example shows how to enable NTP on a VDC:

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

This example shows how to disable NTP on a VDC:

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ntp master</b>	Configures the device to act as an authoritative NTP server.
<b>ntp enable</b>	Enables the NTP feature on a VDC.



# feature ptp

To enable the Precision Time Protocol (PTP) feature on the current virtual device context (VDC), 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.

**Defaults** Disabled

**Command Modes** Global configuration mode

**SupportedUserRoles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to enable the PTP feature on the current VDC:

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

This example shows how to disable the PTP feature on the current VDC:

```
switch(config)# no feature ptp
2011 Jul 5 06:11:07 switch %FEATURE-MGR-2-FM_AUTOCKPT_IN_PROGRESS: AutoCheckpoi
nt system-fm-ntp's creation in progress...
2011 Jul 5 06:11:07 switch %FEATURE-MGR-2-FM_AUTOCKPT_SUCCEEDED: AutoCheckpoint
created successfully
switch(config)#
```

Related Commands	Command	Description
	<b>ntp source</b>	Configures the source IP address for all PTP packets.
	<b>ntp domain</b>	Configures the domain number to use for this clock.
	<b>ntp priority1</b>	Configures the priority1 value to use when advertising this clock.

<b>Command</b>	<b>Description</b>
<b>ptp priority2</b>	Configures the priority2 value to use when advertising this clock.
<b>show ptp brief</b>	Displays the PTP status.
<b>show ptp clock</b>	Displays the properties of the local clock.

# feature scheduler

To enable the scheduling of maintenance jobs, use the **feature scheduler** command. To disable the scheduler, 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

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modified
	4.0(1)	This command was introduced.

**Usage Guidelines** You must enable the scheduler feature before you can configure a maintenance job. Maintenance jobs can be scheduled for one-time-only or at periodic intervals. Maintenance jobs include quality of service policy changes, data and configuration backup, and so on. This command does not require a license.

**Examples** This example shows how to enable the scheduler:

```
switch# config t
switch(config)# feature scheduler
switch(config)#
```

This example shows how to disable the scheduler:

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

Related Commands	Command	Description
	<b>scheduler</b>	Creates and schedules maintenance jobs.
	<b>show scheduler</b>	Displays scheduler information.

# filesys delete

To delete a specific file in the /var/tmp directory, use the filesys delete command.

```
filesys delete /var/tmp/file-name
```

## Syntax Description

<i>file-name</i>	The complete filename.
------------------	------------------------

## Defaults

None

## Command Modes

Any command mode

## Supported User Roles

network-admin  
vdc-admin  
network-operator  
vdc-operator

## Command History

Release	Modified
4.2(4)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to delete a specific file from the /var/tmp directory:

```
switch# filesys delete /var/tmp/abc.log
Please Wait.File is being deleted.
Successfully deleted the file.
switch#
```

## filter (ERSPAN)

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

```
filter [access-group acl-filter] [vlan vlan-range] [bpdu [true | false]] [cos cos-value] [dest-mac
dest-mac] [eth-type eth-value] [flow-hash flow-value] [pc-lane port-number] [src_mac
mac-address] [trace-route [true | false]]
```

```
no filter [access-group acl-filter] [vlan vlan-range] [bpdu [true | false]] [cos cos-value] [dest-mac
dest-mac] [eth-type eth-value] [flow-hash flow-value] [pc-lane port-number] [src_mac
mac-address] [trace-route [true | false]]
```

Syntax Description	
<b>access-group</b> <i>acl-filter</i>	(Optional) Specifies a filter based on an access control group.
<b>vlan</b> <i>vlan-range</i>	(Optional) Specifies a filter based on a VLAN range.
<b>bpdu</b>	(Optional) Specifies a filter based on the bridge protocol data unit (BPDU) class of packets.
<b>true</b>	(Optional) Specifies that a filter based on the bridge protocol data unit (BPDU) class of packets is used.
<b>false</b>	(Optional) Specifies a filter based on non-BPDU class of packets.
<b>cos</b> <i>cos-value</i>	(Optional) Specifies a filter based on the class of service (CoS) in the dot1q header.
<b>dest-mac</b> <i>dest-mac</i>	(Optional) Specifies a filter based on a destination MAC address.
<b>eth-type</b> <i>eth-value</i>	(Optional) Specifies a filter based on the Ethernet type.
<b>flow-hash</b> <i>flow-value</i>	(Optional) Specifies a filter based on the result bundle hash (RBH) value.
<b>pc-lane</b> <i>port-number</i>	(Optional) Specifies a filter based on a member of the port channel.
<b>src_mac</b> <i>mac-address</i>	(Optional) Specifies a filter based on a source MAC address.
<b>trace-route</b>	(Optional) Specifies a filter based on trace-route packets.
<b>true</b>	(Optional) Specifies a that a filter based on trace-route packets is used.
<b>false</b>	(Optional) Specifies a filter based on non trace-route packets.

**Defaults** None

**Command Modes** config-erspan-src mode

**SupportedUserRoles** network-admin  
VDC-admin

## filter (ERSPAN)

### Command History

Release	Modification
6.2(2)	This command was introduced.

### Usage Guidelines

You can configure filters for ingress or egress ERSPAN traffic based on a set of rules. A simple filter has only one rule, and multiple fields or conditions can be added to this rule. The packets are spanned only if all conditions are met.

Port channel member lane is not supported on F1 Series modules.

F2 and F2e Series modules do not support egress SPAN filtering for destination MAC addresses and source MAC addresses.

This command does not require a license.

### Examples

This example shows how to configure filters for an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# filter vlan 3-5
switch(config-erspan-src)# filter trace-route true
```

### Related Commands

Command	Description
<b>filter (SPAN)</b>	Configures the filters for a SPAN session.

## filter (SPAN)

To configure the filters for an Ethernet Switched Port Analyzer (SPAN) session, use the **filter** command. To remove the filters, use the **no** form of this command.

```
filter [vlan vlan-range] [bpdu [true | false]] [cos cos-value] [dest-mac dest-mac] [eth-type
eth-value] [flow-hash flow-value] [pc-lane port-number] [src_mac mac-address] [trace-route
[true | false]]
```

```
no filter [vlan vlan-range] [bpdu [true | false]] [cos cos-value] [dest-mac dest-mac] [eth-type
eth-value] [flow-hash flow-value] [pc-lane port-number] [src_mac mac-address] [trace-route
[true | false]]
```

Syntax Description		
<b>vlan</b> <i>vlan-range</i>	(Optional)	Specifies a filter based on a VLAN range.
<b>bpdu</b>	(Optional)	Specifies a filter based on the bridge protocol data unit (BPDU) class of packets.
<b>true</b>	(Optional)	Specifies that a filter based on the bridge protocol data unit (BPDU) class of packets is used.
<b>false</b>	(Optional)	Specifies a filter based on non-BPDU class of packets.
<b>cos</b> <i>cos-value</i>	(Optional)	Specifies a filter based on the class of service (CoS) in the dot1q header.
<b>dest-mac</b> <i>dest-mac</i>	(Optional)	Specifies a filter based on a destination MAC address.
<b>eth-type</b> <i>eth-value</i>	(Optional)	Specifies a filter based on the Ethernet type.
<b>flow-hash</b> <i>flow-value</i>	(Optional)	Specifies a filter based on the result bundle hash (RBH) value.
<b>pc-lane</b> <i>port-number</i>	(Optional)	Specifies a filter based on a member of the port channel.
<b>src_mac</b> <i>mac-address</i>	(Optional)	Specifies a filter based on a source MAC address.
<b>trace-route</b>	(Optional)	Specifies a filter based on trace-route packets.
<b>true</b>	(Optional)	Specifies a that a filter based on trace-route packets is used.
<b>false</b>	(Optional)	Specifies a filter based on non trace-route packets.

**Defaults** None

**Command Modes** Config-monitor configuration mode (config-monitor)

**SupportedUserRoles** network-admin  
VDC-admin

Command History	Release	Modification
	6.2(2)	This command was introduced.

**Usage Guidelines**

You can configure filters for ingress or egress SPAN traffic based on a set of rules. A simple filter has only one rule, and multiple fields or conditions can be added to this rule. The packets are spanned only if all conditions are met.

Port channel member lane is not supported on F1 Series modules.

F2 and F2e Series modules do not support egress SPAN filtering for destination MAC addresses and source MAC addresses.

This command does not require a license.

**Examples**

This example shows how to configure filters for an SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# filter vlan 3-5
switch(config-monitor)# filter trace-route true
```

**Related Commands**

Command	Description
<b>filter (ERSPAN)</b>	Configures the filters for an ERSPAN session.
<b>show monitor session</b>	Displays information about a SPAN or ERSPAN session.



# filter access-group

To apply an access group to an Encapsulated Remote Switched Port Analyzer (ERSPAN) source session, use the **filter access-group** command. To remove an access group, use the **no** form of this command.

**filter access-group** *acl\_filter*

**no filter access-group** *acl\_filter*

<b>Syntax Description</b>	<i>acl_filter</i>	Access control list (ACL) name. An ACL associates the access list with the SPAN session.
---------------------------	-------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	config-monitor-erspan-src
----------------------	---------------------------

<b>SupportedUserRoles</b>	network-admin VDC-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.1(1)	This command was introduced.

<b>Usage Guidelines</b>	<p>Only the permit to deny actions are allowed for Encapsulated Remote Switched Port Analyzer (ERSPAN) access control list (ACL) filters.</p> <p>For information about ACL-related commands, see the <i>Cisco Nexus 7000 Series NX-OS Security Command Reference</i>.</p> <p>This command does not require a license.</p>
-------------------------	---

<b>Examples</b>	This example shows how to apply an access group to an ERSPAN session:
-----------------	---

```
switch# configure terminal
switch(config)# monitor session 3 type erspan-source
switch(config-monitor-erspan-src)# filter vlan 3-5, 7
switch(config-monitor-erspan-src)# filter access-group ACL1
```

This example shows how to disassociate an access group to an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 3 type erspan-source
switch(config-monitor-erspan-src)# filter vlan 3-5, 7
switch(config-monitor-erspan-src)# no filter access-group ACL1
```

## ■ filter access-group

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>filter vlan</b>	Applies a VLAN filter to a session.

## filter frame-type arp

To configure the Address Resolution Protocol (ARP) frame type filter for the Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **filter frame-type arp** command. To remove the filter from the session, enter the **no** form of this command.

```
filter frame-type arp [arp-rarp [arp | rarp] [req-resp [req | rsp]] [sender-ip ip-address]
[target-ip ip-address]]
```

```
no filter frame-type arp [arp-rarp [arp | rarp] [req-resp [req | rsp]] [sender-ip ip-address]
[target-ip ip-address]]
```

Syntax Description		
<b>arp-rarp</b>	(Optional) Specifies an ARP or Reverse Address Resolution Protocol (RARP) frame type filter.	
<b>arp</b>	(Optional) Specifies an ARP frame type filter.	
<b>rarp</b>	(Optional) Specifies an RARP frame type filter.	
<b>req-resp</b>	(Optional) Specifies a filter based on a request or response.	
<b>req</b>	(Optional) Specifies a filter based on a request.	
<b>resp</b>	(Optional) Specifies a filter based on a response.	
<b>sender-ip</b> <i>ip-address</i>	(Optional) Specifies a filter based on a sender IP address.	
<b>target-ip</b> <i>ip-address</i>	(Optional) Specifies a filter based on a target IP address.	

**Defaults** None

**Command Modes** config-erspan-src mode

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	6.2(2)	This command was introduced.

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

**Examples** This example shows how to configure the ARP frame type filter for the ERSPAN session:

```
switch(config)# monitor session 1 type erspan-source  
switch(config-erspan-src)# filter frame-type arp arp-rarp arp
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>filter (ERSPAN)</b>	Configures the filters for an ERSPAN session.
<b>filter frame-type eth</b>	Configures the Ethernet frame type filter for the SPAN or ERSPAN session.
<b>filter frame-type fcoe</b>	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
<b>filter frame-type ipv4</b>	Configures the IPv4 frame type filter for the SPAN or ERSPAN session.
<b>filter frame-type ipv6</b>	Configures the IPv6 frame type filter for the SPAN or ERSPAN session.
<b>monitor session</b>	Places you in the monitor configuration mode for configuring a SPAN or ERSPAN session.

# filter frame-type eth

To configure the Ethernet frame type filter for the Ethernet Switched Port Analyzer (SPAN) or Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **filter frame-type eth** command. To remove the Ethernet frame type filter, use the **no** form of this command.

**filter frame-type eth**

**no filter frame-type eth**

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

**Command Modes** config-monitor mode (for a SPAN session)  
config-erspan-src mode (for an ERSPAN session)

**Supported User Roles** network-admin  
vdc-admin

Command History	Release	Modification
	6.2(2)	This command was introduced.

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

**Examples** This example shows how to configure the Ethernet frame type filter for a SPAN session:

```
switch(config)# monitor session 1
switch(config-monitor)# filter frame-type eth
```

This example shows how to configure the Ethernet frame type filter for an ERSPAN session:

```
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter frame-type eth
```

Related Commands	Command	Description
	<b>filter (ERSPAN)</b>	Configures the filters for an ERSPAN session.
	<b>filter (SPAN)</b>	Configures the filters for a SPAN session.
	<b>filter frame-type arp</b>	Configures the ARP frame type filter for the ERSPAN session.
	<b>filter frame-type fcoe</b>	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
	<b>filter frame-type ipv4</b>	Configures the IPv4 frame type filter for the SPAN or ERSPAN session.

Command	Description
<b>filter frame-type ipv6</b>	Configures the IPv6 frame type filter for the SPAN or ERSPAN session.
<b>monitor session</b>	Places you in the monitor configuration mode for configuring a SPAN or ERSPAN session.

# filter frame-type fcoe

To configure the Fibre Channel over Ethernet (FCoE) frame type filter for the Ethernet Switched Port Analyzer (SPAN) or Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **filter frame-type fcoe** command. To remove the FCoE frame type filter, use the **no** form of this command.

```
filter frame-type fcoe [[fc-sid FC-source-ID] [fc-did FC-dest-ID] [fcoe-type fcoe-value] [r-ctl r-ctl-value] [sof sof-value] [cmd-code cmd-value]]
```

```
no filter frame-type fcoe [[fc-sid FC-source-ID] [fc-did FC-dest-ID] [fcoe-type fcoe-value] [r-ctl r-ctl-value] [sof sof-value] [cmd-code cmd-value]]
```

Syntax Description		
<b>fc-sid</b> <i>FC-source-ID</i>	(Optional)	Specifies a filter based on an FC source ID.
<b>fc-did</b> <i>FC-dest-ID</i>	(Optional)	Specifies a filter based on an FC destination ID.
<b>fcoe-type</b> <i>fcoe-value</i>	(Optional)	Specifies a filter based on an FCoE type.
<b>r-ctl</b> <i>r-ctl-value</i>	(Optional)	Specifies a filter based on the routing control flags (R CTL) value.
<b>sof</b> <i>sof-value</i>	(Optional)	Specifies a filter based on the start of frame (SOF) packets.
<b>cmd-code</b> <i>cmd-value</i>	(Optional)	Specifies a filter based on a command code.

**Defaults** None

**Command Modes** config-monitor mode (for a SPAN session)  
config-erspan-src mode (for an ERSPAN session)

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	6.2(2)	This command was introduced.

**Usage Guidelines** F1 Series modules do not support FCoE source IDs and FCoE destination IDs.  
This command does not require a license.

**Examples** This example shows how to configure the FCoE frame type filter for a SPAN session:

```
switch(config)# monitor session 1  
switch(config-monitor)# filter frame-type fcoe
```

This example shows how to configure the FCoE frame type filter for an ERSPAN session:

```
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter frame-type fcoe fc-did 2
```

#### Related Commands

Command	Description
<b>filter (ERSPAN)</b>	Configures the filters for an ERSPAN session.
<b>filter (SPAN)</b>	Configures the filters for a SPAN session.
<b>filter frame-type arp</b>	Configures the ARP frame type filter for the ERSPAN session.
<b>filter frame-type eth</b>	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
<b>filter frame-type ipv4</b>	Configures the IPv4 frame type filter for the SPAN or ERSPAN session.
<b>filter frame-type ipv6</b>	Configures the IPv6 frame type filter for the SPAN or ERSPAN session.
<b>monitor session</b>	Places you in the monitor configuration mode for configuring a SPAN or ERSPAN session.



# filter frame-type ipv4

To configure the IPv4 frame type filter for the Ethernet Switched Port Analyzer (SPAN) or Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **filter frame-type ipv4** command. To remove the Ethernet frame type filter, use the **no** form of this command.

```
filter frame-type ipv4 [[src-ip src-ip] [dest-ip dest-ip] [tos tos-value] [l4-protocol l4-value]]
```

```
no filter frame-type ipv4 [[src-ip src-ip] [dest-ip dest-ip] [tos tos-value] [l4-protocol l4-value]]
```

## Syntax Description

<b>src-ip</b> <i>src-ip</i>	(Optional) Specifies a filter based on an IPv4 source IP address.
<b>dest-ip</b> <i>dest-ip</i>	(Optional) Specifies a filter based on an IPv4 destination IP address.
<b>tos</b> <i>tos-value</i>	(Optional) Specifies a filter based on the type of service (ToS) in the IP header.
<b>l4-protocol</b> <i>l4-value</i>	(Optional) Specifies a filter based on a Layer 4 protocol number set in the protocol field of the IP header.

## Defaults

None

## Command Modes

config-monitor mode (for a SPAN session)  
 config-erspan-src mode (for an ERSPAN session)

## Supported User Roles

network-admin  
 vdc-admin

## Command History

Release	Modification
6.2(2)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure the IPv4 frame type filter for a SPAN session:

```
switch(config)# monitor session 1  
switch(config-monitor)# filter frame-type ipv4 l4-protocol 3
```

This example shows how to configure the IPv4 frame type filter for an ERSPAN session:

```
switch(config)# monitor session 1 type erspan-source  
switch(config-erspan-src)# filter frame-type ipv4 l4-protocol 3
```

Related Commands	Command	Description
	<b>monitor session</b>	Places you in the monitor configuration mode for configuring a SPAN or ERSPAN session.
	<b>filter (ERSPAN)</b>	Configures the filters for an ERSPAN session.
	<b>filter (SPAN)</b>	Configures the filters for a SPAN session.
	<b>filter frame-type arp</b>	Configures the ARP frame type filter for the ERSPAN session.
	<b>filter frame-type eth</b>	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
	<b>filter frame-type fcoe</b>	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
	<b>filter frame-type ipv6</b>	Configures the IPv6 frame type filter for the SPAN or ERSPAN session.

## filter frame-type ipv6

To configure the IPv6 frame type filter for the Ethernet Switched Port Analyzer (SPAN) or Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **filter frame-type ipv6** command. To remove the IPv6 frame type filter, use the **no** form of this command.

```
filter frame-type ipv6 [src-ip src-ip] [dest-ip dest-ip] [tos tos-value] [I4-protocol l4-value]
```

```
no filter frame-type ipv6 [src-ip src-ip] [dest-ip dest-ip] [tos tos-value] [I4-protocol l4-value]
```

### Syntax Description

<b>src-ip</b> <i>src-ip</i>	(Optional) Specifies a filter based on an IPv6 source IP address.
<b>dest-ip</b> <i>dest-ip</i>	(Optional) Specifies a filter based on an IPv6 destination IP address.
<b>tos</b> <i>tos-value</i>	(Optional) Specifies a filter based on the type of service (ToS) in the IP header.
<b>I4-protocol</b> <i>l4-value</i>	(Optional) Specifies a filter based on a Layer 4 protocol number set in the protocol field of the IP header.

### Defaults

None

### Command Modes

config-monitor mode (for a SPAN session)  
config-erspan-src mode (for an ERSPAN session)

### Supported User Roles

network-admin  
vdc-admin

### Command History

Release	Modification
6.2(2)	This command was introduced.

### Usage Guidelines

F1 Series modules have limited support for rule-based SPAN. They do not support IPv6 source IP and IPv6 destination IP filters. They support only IPv4 and IPv6 ToS filters with values from 0 to 3.

F2 and F2e Series modules have limited support for rule-based SPAN. They do not support wildcards in the IPv6 source IP filter and IPv6 destination IP filter.

This command does not require a license.

### Examples

This example shows how to configure the IPv6 frame type filter for a SPAN session:

```
switch(config)# monitor session 1  
switch(config-monitor)# filter frame-type ipv6 src-ip 10.0.0.1
```

This example shows how to configure the IPv6 frame type filter for an ERSPAN session:

```
switch(config)# monitor session 1 type erspan-source  
switch(config-erspan-src)# filter frame-type ipv6 src-ip 10.0.0.1
```

Related Commands	Command	Description
	<b>monitor session</b>	Places you in the monitor configuration mode for configuring a SPAN or ERSPAN session.
	<b>filter (ERSPAN)</b>	Configures the filters for an ERSPAN session.
	<b>filter (SPAN)</b>	Configures the filters for a SPAN session.
	<b>filter frame-type arp</b>	Configures the ARP frame type filter for the ERSPAN session.
	<b>filter frame-type eth</b>	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
	<b>filter frame-type fcoe</b>	Configures the FCoE frame type filter for the SPAN or ERSPAN session.
	<b>filter frame-type ipv4</b>	Configures the IPv4 frame type filter for the SPAN or ERSPAN session

# filter vlan

To apply a VLAN access map to one or more VLANs, use the **filter vlan** command. To remove a VLAN access map, use the **no** form of this command.

**filter vlan** *vlan\_mrange* [**include-untagged**]

**no filter vlan** *vlan\_mrange* [**include-untagged**]

<b>Syntax Description</b>	<i>vlan_mrange</i>	Name of the VLAN access map that you want to create or configure. The range is from 1 to 3967 and from 4048 to 4093.
	<b>include-untagged</b>	(Optional) Specifies untagged frames on a port with Layer 3 subinterfaces.

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Config-monitor configuration (config-monitor)
----------------------	---

<b>Supported User Roles</b>	network-admin vdc-admin
-----------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to apply a VLAN access map to one or more VLANs:

```
switch(config)# monitor session 1
switch(config-monitor)# filter vlan 5-10 include-untagged
switch(config-monitor)#
```

This example shows how to remove the VLAN access map:

```
switch(config-monitor)# no filter vlan 5-10 include-untagged
switch(config-monitor)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>filter vlan include-untagged</b>	Applies a VLAN access map to one or more VLANs and includes untagged frames on a port with Layer 3 subinterfaces.

# filter vlan include-untagged

To apply a VLAN access map to one or more VLANs and include untagged frames on a port with Layer 3 subinterfaces, use the **filter vlan include-untagged** command. To remove a VLAN access map to one or more VLANs with untagged frames on a port with Layer 3 subinterfaces, use the **no** form of this command.

**filter vlan include-untagged**

**no filter vlan include-untagged**

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

**Defaults** None

**Command Modes** Config-monitor configuration (config-monitor)

**Supported User Roles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to apply a VLAN access map to one or more VLANs and include untagged frames on a port with Layer 3 subinterfaces:

```
switch(config)# monitor session 1
switch(config-monitor)# filter vlan 1-20 include-untagged
switch(config-monitor)#
```

This example shows how to remove a VLAN access map to one or more VLANs with untagged frames on a port with Layer 3 subinterfaces:

```
switch(config-monitor)# no filter vlan 1-20 include-untagged
switch(config-monitor)#
```

Related Commands	Command	Description
	<b>filter vlan</b>	Applies a VLAN access map to one or more VLANs.

# flow exporter

To create a Flexible NetFlow flow exporter or to modify an existing Flexible NetFlow flow exporter, use the **flow exporter** command. To remove a Flexible NetFlow flow exporter, use the **no** form of this command.

**flow exporter** *exporter-name*

**no flow exporter** *exporter-name*

## Syntax Description

<i>exporter-name</i>	Name of the flow exporter that is created or modified.
----------------------	--

## Defaults

Flow exporters are not present in the configuration until you create them.

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.

Once you enter the flow export configuration mode, the prompt changes to the following:

```
switch(config-flow-exporter)#
```

Within the flow export configuration mode, the following keywords and arguments are available to configure the flow exporters:

- **description** *description*—Provides a description for this flow exporter; you can use a maximum of 63 characters.
- **destination** {*ip-addr* | *ipv6-addr*} [**use-vrf** *label-name*]—Specifies the destination address for the collector. Enter the optional **use-vrf** *label-name* to specify a VRF. Use the following format when entering the destination address:
  - *ip-addr*—*A.B.C.D*
  - *ipv6-addr*—*A:B::C:D*

- **dscp** *value*—Specifies the differentiated services code point (DSCP) value. The range is from 0 to 63.
- **exit**—Exits from the current configuration mode.
- **no**—Negates a command or sets its defaults.
- **source** *interface*—Specifies the source interface for this destination. The valid values for *interface* are as follows:
  - **ethernet** *mod/port*—Specifies the Ethernet IEEE 802.3z interface module and port number. The ranges for the module and port number depend on the chassis used.
  - **loopback** *virtual-num*—Specifies the virtual interface number. The range is from 0 to 1023.
  - **mgmt** *num*—Specifies the management interface number. The range is from 0 to 10.
- **transport udp** *dest-port*—Specifies the transport UDP destination port. The range is from 0 to 65535.
- **version** {5 | 9}—Specifies the export version 5 or the version 9 and enters the export version configuration mode. See the **version** command for additional information.

This command does not require a license.

## Examples

This example shows how to create a flow exporter named FLOW-EXPORTER-1, enter flow exporter configuration mode, and configure the flow exporter:

```
switch(config)# flow exporter FLOW-EXPORTER-1
switch(config-flow-exporter)# description located in Pahrump, NV
switch(config-flow-exporter)# destination A.B.C.D
switch(config-flow-monitor)# dscp 32
switch(config-flow-monitor)# source ethernet 3/2
switch(config-flow-monitor)# transport udp 59
switch(config-flow-monitor)# version 5
```

## Related Commands

Command	Description
<b>clear flow exporter</b>	Clears the flow monitor.
<b>show flow exporter</b>	Displays flow monitor status and statistics.



# flow monitor

To create a Flexible NetFlow flow monitor or to modify an existing Flexible NetFlow flow monitor and enter flow monitor configuration mode, use the **flow monitor** command. To remove a Flexible NetFlow flow monitor, use the **no** form of this command.

**flow monitor** *monitor-name*

**no flow monitor** *monitor-name*

## Syntax Description

<i>monitor-name</i>	Name of the flow monitor that is created or modified.
---------------------	---

## Defaults

Flow monitors are not present in the configuration until you create them.

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

Flow monitors are the Flexible NetFlow component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a record that you add to the flow monitor after you create the flow monitor and a cache that is automatically created at the time that the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in record that is configured for the flow monitor and stored in the flow monitor cache.

Once you enter the flow monitor configuration mode, the prompt changes to the following:

```
switch(config-flow-monitor)#
```

Within the flow monitor configuration mode, the following keywords and arguments are available to configure the flow monitor:

- **description** *description*—Provides a description for this flow monitor; you use a maximum of 63 characters.
- **exit**—Exits from the current configuration mode.
- **exporter** *name*—Specifies the name of an exporter to export records.
- **no**—Negates a command or sets its defaults.
- **record** {*record-name* | **netflow ipv4** *collection-type* | **netflow-original**}—Specifies a flow record to use as follows:

- *record-name*—Name of a record.
- **netflow ipv4 collection-type**—Specifies the traditional IPv4 NetFlow collection schemes as follows:
  - original-input**—Specifies the traditional IPv4 input NetFlow.
  - original-output**—Specifies the traditional IPv4 output NetFlow.
  - protocol-port**—Specifies the protocol and ports aggregation scheme.
- **netflow-original**—Specifies the traditional IPv4 input NetFlow with origin autonomous systems.

The **netflow-original** and **original-input** keywords are the same and are equivalent to the following commands:

- **match ipv4 source address**
- **match ipv4 destination address**
- **match ip tos**
- **match ip protocol**
- **match transport source-port**
- **match transport destination-port**
- **match interface input**
- **collect counter bytes**
- **collect counter packet**
- **collect timestamp sys-uptime first**
- **collect timestamp sys-uptime last**
- **collect interface output**
- **collect transport tcp flags**
- **collect routing next-hop address ipv4**
- **collect routing source as**
- **collect routing destination as**

The **original-output** keywords are the same as the **original-input** keywords except for the following:

- **match interface output** (instead of **match interface input**)
- **collect interface input** (instead of **collect interface output**)

This command does not require a license.

## Examples

This example shows how to create and configure a flow monitor named FLOW-MONITOR-1:

```
switch(config)# flow monitor FLOW-MONITOR-1
switch(config-flow-monitor)# description monitor location las vegas, NV
switch(config-flow-monitor)# exporter exporter-name1
switch(config-flow-monitor)# record test-record
switch(config-flow-monitor)# netflow ipv4 original-input
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear flow monitor</b>	Clears the flow monitor.
<b>show flow sw-monitor</b>	Displays flow monitor status and statistics.

# flow record

To create a Flexible NetFlow flow record or to modify an existing Flexible NetFlow flow record and enter flow record configuration mode, use the **flow record** command. To remove a Flexible NetFlow flow record, use the **no** form of this command.

**flow record** *record-name*

**no flow record** *record-name*

## Syntax Description

<i>record-name</i>	Name of the flow record that is created or modified.
--------------------	--

## Defaults

Flow records are not present in the configuration until you create them.

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

Flexible NetFlow uses key and nonkey fields just as original NetFlow does to create and populate flows in a cache. In Flexible NetFlow, a combination of key and nonkey fields is called a record. Original NetFlow and Flexible NetFlow both use the values in key fields in IP datagrams, such as the IP source or destination address and the source or destination transport protocol port, as the criteria for determining when a new flow must be created in the cache while network traffic is being monitored. A flow is defined as a stream of packets between a given source and a given destination. New flows are created whenever NetFlow analyzes a packet that has a unique value in one of the key fields.

Once you enter the flow record configuration mode, the prompt changes to the following:

```
switch(config-flow-record) #
```

Within the flow record configuration mode, the following keywords and arguments are available to configure the flow record:

- **collect**—Specifies a nonkey field. See the **collect** command for additional information.
- **description** *description*—Provides a description for this flow record; you use a maximum of 63 characters.
- **exit**—Exits from the current configuration mode.
- **match**—Specifies a key field. See the **match** command for additional information.
- **no**—Negates a command or sets its defaults.

Cisco NX-OS enables the following match fields by default when you create a flow record:

- **match interface input**
- **match interface output**
- **match flow direction**

This command does not require a license.

### Examples

This example shows how to create a flow record and enter flow record configuration mode:

```
switch(config)# flow record FLOW-RECORD-1  
switch(config-flow-record)#
```

### Related Commands

Command	Description
<b>clear flow monitor</b>	Clears the flow monitor.
<b>flow monitor</b>	Creates a flow monitor.
<b>show flow sw-monitor</b>	Displays flow monitor status and statistics.

# flow timeout

To create a Flexible NetFlow flow timeout or to modify an existing Flexible NetFlow flow timeout, use the **flow timeout** command. To remove a Flexible NetFlow flow timeout, use the **no** form of this command.

**flow timeout** { **active** *seconds* | **aggressive threshold** *percentage* | **fast** *seconds* **threshold** *packets* | **inactive** *seconds* | **session** | *seconds* }

**no flow timeout** { **active** *seconds* | **aggressive threshold** *percentage* | **fast** *seconds* **threshold** *packets* | **inactive** *seconds* | **session** | *seconds* }

## Syntax Description

<b>active</b> <i>seconds</i>	Specifies the active or long timeout in seconds. The range is from 60 to 4092. The default is 1800.
<b>aggressive threshold</b> <i>percentage</i>	Specifies the percentage of the NetFlow table content. The range is from 50 to 99.
<b>fast</b> <i>seconds</i>	Specifies the fast aging timeout in seconds. The range is from 32 to 512. The default is not supported.
<b>threshold</b> <i>packets</i>	Specifies the packet threshold for a flow timeout in packets. The range is from 1 to 4000. The default is not supported.
<b>inactive</b> <i>seconds</i>	Specifies the inactive or normal timeout in seconds. The range is from 15 to 4092. The default is 15.
<b>session</b>	Enables TCP session aging.
<i>seconds</i>	Flush timeout value in seconds for F2 Series modules. The range is from 5 to 60 seconds.

## Defaults

The default settings are as follows:

- Active timeout—1800 seconds
- Aggressive aging timeout—Disabled
- Fast timeout—Disabled
- Inactive timeout—15 seconds
- Session aging timeout—Disabled
- Flush cache timeout – 15 seconds (enabled only on F2)

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

**Command History**

Release	Modification
6.1(2)	Added the <i>seconds</i> argument for the syntax description and also the note.
4.0(1)	This command was introduced.

**Usage Guidelines**

The active timeout is the amount of time to wait before sending flow information about an active session. The flow is not removed from the cache after this timeout; however, the packet count, byte count, and timestamps are reset.

The aggressive timeout only affects hardware caches and is used when flows are being received faster than expected. If flows are being received faster than the threshold, they are aged out of the cache.

The fast timeout specifies when an inactive flow should be aged out.

The inactive timeout is used for Transmission Control Protocol (TCP) sessions that receive no more data from the sender (FIN) followed by an acknowledgment field is significant (ACK) or a reset (RST) packet being received. The inactive timeout indicates the session is over and the flow can be aged out.

**Note**

Only the flow timeout seconds command is supported for F2 Series modules. All of the other NetFlow timeout commands are supported for M Series modules only.

This command does not require a license.

**Examples**

This example shows how to specify the active or long timeout value in seconds for the F1 and M1 Series modules:

```
switch(config)# flow timeout active 45
switch(config)#
```

This example shows how to specify the percentage of the NetFlow table content:

```
switch(config)# flow timeout aggressive threshold 45
switch(config)#
```

This example shows how to specify the fast aging timeout in seconds:

```
switch(config)# flow timeout fast 30 threshold 20
switch(config)#
```

This example shows how to specify the inactive or normal timeout in seconds:

```
switch(config)# flow timeout inactive 45
switch(config)#
```

This example shows how to specify the flush cache timeout in seconds for F2 Series module:

```
switch(config)# flow timeout 45
switch(config)#
```

**Related Commands**

Command	Description
<b>flow record</b>	Creates a flow exporter.
<b>clear flow monitor</b>	Clears the flow monitor.

Command	Description
<b>flow monitor</b>	Creates a flow monitor.
<b>show flow sw-monitor</b>	Displays flow monitor status and statistics.





# H Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter H.

# hardware fan-tray maintenance-mode

To put the switch in fan tray maintenance mode to prepare the switch for fan tray migration or removal, use the **hardware fan-tray maintenance-mode** command. To disable fan tray maintenance mode, use the **no** form of this command.

**hardware fan-tray maintenance-mode** [**long** | **medium** | **short**]

**no hardware fan-tray maintenance-mode** [**long** | **medium** | **short**]

## Syntax Description

<b>long</b>	(Optional) The fans run at 65% speed for approximately 9 minutes.
<b>medium</b>	(Optional) The fans run at 75% speed for approximately 6 minutes.
<b>short</b>	(Optional) The fans run at 85% speed for approximately 4 minutes.

## Defaults

The fans run at 100% speed for approximately 4 minutes. Starting from Cisco NX-OS Release 8.1(1), the fans run at 85% speed for approximately 4 minutes.

## Command Modes

Global configuration mode (config)

## Supported User Roles

network-admin  
vdc-admin  
network-operator  
vdc-operator

## Command History

Release	Modification
8.1(1)	This command was modified. By default, the fans will now run at 85% speed for approximately 4 minutes when the <b>hardware fan-tray maintenance-mode</b> command is used.
7.2(0)D1(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

The fan tray maintenance mode will be cancelled in the following cases:

- If a temperature alarm is present.
- Hot-inlet temperature (Sup inlet temperature  $\geq$  30 degrees Celsius)
- A fan tray is absent.
- Post-cool period (time elapsed after fan tray removal) has crossed 4 minutes.

**Note**

The fan tray maintenance mode is cancelled and the fan speed will be set to normal if the fan tray migration or replacement has been completed within 2 minutes after using the **hardware fan-tray maintenance-mode** command. If the fan tray migration or replacement has not been completed within 2 minutes, the remaining fan trays run at 85% speed for the next 2 minutes and at 100% speed from then on.

- Pre-cool period has crossed 1 hour and 9 minutes - The fan tray has not been removed since the past 1 hour and 9 minutes during which the switch was ready for fan tray removal.

**Examples**

This example shows how to prepare the switch for fan tray removal or migration by putting the switch in fan tray maintenance mode and making the fans run at 85% speed for approximately 4 minutes:

```
switch# configure terminal
switch(config)# hardware fan-tray maintenance-mode
2017 Apr 7 16:11:04 SWITCH %PLATFORM-6-PFM_INFO: Fan Zone 1 : Fan Speed will change from
37.25(0x5f) to 85.10(0xd9)
```

This example shows how to prepare the switch for fan tray removal or migration by putting the switch in fan tray maintenance mode and making the fans run at 65% speed for approximately 9 minutes:

```
switch# configure terminal
switch(config)# hardware fan-tray maintenance-mode long
2017 Apr 3 19:07:07 SWITCH %PLATFORM-6-PFM_INFO: Fan Zone 1 : Fan Speed will change from
45.88(0x75) to 65.10(0xa6)
2017 Apr 3 19:07:07 SWITCH %PLATFORM-2-PFM_CRITICAL: FAN_MAINTENANCE_MODE: Fan maintenance
mode started.
Please wait for 4-9 minutes for precool to complete before replacing the FANs
2017 Apr 3 19:16:09 SWITCH %PLATFORM-2-PFM_CRITICAL: FAN_MAINTENANCE_MODE: system is ready
for fan-removal.
```

This example shows how to prepare the switch for fan tray removal or migration by putting the switch in fan tray maintenance mode and making the fans run at 75% speed for approximately 6 minutes:

```
switch# configure terminal
switch(config)# hardware fan-tray maintenance-mode medium
2017 Apr 3 18:58:19 SWITCH %PLATFORM-6-PFM_INFO: Fan Zone 1 : Fan Speed will change from
45.88(0x75) to 74.90(0xbf)
2017 Apr 3 18:58:19 SWITCH %PLATFORM-2-PFM_CRITICAL: FAN_MAINTENANCE_MODE: Fan maintenance
mode started.
Please wait for 4-9 minutes for precool to complete before replacing the FANs
2017 Apr 3 19:04:20 SWITCH %PLATFORM-2-PFM_CRITICAL: FAN_MAINTENANCE_MODE: system is ready
for fan-removal.
```

This example shows how to prepare the switch for fan tray removal or migration by putting the switch in fan tray maintenance mode and making the fan run at 85% speed for approximately 4 minutes:

```
switch# configure terminal
switch(config)# hardware fan-tray maintenance-mode short
2017 Apr 3 19:16:41 SWITCH %PLATFORM-6-PFM_INFO: Fan Zone 1 : Fan Speed will change from
45.88(0x75) to 85.10(0xd9)
2017 Apr 3 19:16:41 SWITCH %PLATFORM-2-PFM_CRITICAL: FAN_MAINTENANCE_MODE: Fan maintenance
mode started.
Please wait for 4-9 minutes for precool to complete before replacing the FANs
2017 Apr 3 19:20:42 SWITCH %PLATFORM-2-PFM_CRITICAL: FAN_MAINTENANCE_MODE: system is ready
for fan-removal.
```

This example shows how to disable fan tray maintenance mode and change the fan speed from 65% to 45%:

```
switch# configure terminal
switch(config)# no hardware fan-tray maintenance-mode long
2017 Apr 3 19:16:30 SWITCH %PLATFORM-6-PFM_INFO: Fan Zone 1 : Fan Speed will change from
65.10(0xa6) to 45.88(0x75)
```

# hw-module logging onboard

To enable onboard failure logging (OBFL) based on the error type, use the **hw-module logging onboard** command. To disable OBFL (not recommended), use the **no** form of this command.

```
hw-module logging onboard [counter-stats] [environmental-history] [error-stats]
[interrupt-stats] [module num] [obfl-log]
```

```
no hw-module logging onboard [environmental-history] [error-stats] [interrupt-stats] [module
num] [obfl-log]
```

## Syntax Description

<b>counter-stats</b>	(Optional) Specifies the OBFL counter statistics.
<b>environmental-history</b>	(Optional) Specifies the OBFL environmental history.
<b>error-stats</b>	(Optional) Specifies OBFL error statistics.
<b>interrupt-stats</b>	(Optional) Specifies OBFL interrupt statistics.
<b>module num</b>	(Optional) Specifies OBFL information for a specific module.
<b>obfl-log</b>	(Optional) Specifies OBFL (boot-upptime/device-version/obfl-history).

## Defaults

Enabled and is the recommended state.

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(2)	Added <b>counter-stats</b> keyword.

## Usage Guidelines

The **hw-module logging onboard** command enables events to be recorded in files stored in nonvolatile memory, so that the data can be used to diagnose problems with hardware modules installed in a Cisco router or switch. When the onboard hardware is started up, a first record is made for each area monitored and becomes a base value for subsequent records. This command provides a circular updating scheme for collecting continuous records and archiving older (historical) records, ensuring accurate data about the hardware. Data is recorded in one of two formats: continuous information that displays a snapshot of data in a continuous file, and summary information that provides details about the data being collected. Use the **show logging onboard** command to see reports of current and historical data.



### Note

We recommend that you do not disable OBFL.

This configuration command is applicable to the module inserted in a device. When the module is removed and inserted into a new device, the configuration of this command follows the module to the new device.

This command does not require a license.

### Examples

This example shows how to configure OBFL message logging at level 7 (debugging):

```
Router> enable
switch# configure terminal
switch(config)# hw-module switch 2 module 1 logging onboard message level 7
switch(config)# end
```

### Related Commands

Command	Description
<b>attach</b>	Connects to a specific line card for the purpose of executing commands on that card.
<b>clear logging onboard</b>	Clears onboard failure logs.
<b>show logging onboard</b>	Displays onboard failure logs.

# header-type

To set the ERSPAN source version, use the **header-type** command. To disable this feature, use the **no** form of this command.

**header-type** *version*

**no header-type** *version*

Syntax Description	
	<i>version</i> (Optional) specifies the ERSPAN source version 3.

Defaults	
	Enabled and is the recommended state.

Command Modes	
	Global configuration mode

SupportedUserRoles	
	network-admin vdc-admin

Command History	Release	Modification
	6.1(1)	This command was introduced.

Usage Guidelines	
	This command does not require a license.

Examples	
	This example shows how to change the ERSPAN source session from Type II to Type III:

```
switch# configure terminal
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)#
```

Related Commands	Command	Description
	<b>show logging onboard</b>	Displays onboard failure logs.







# I Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter I.

## icam monitor entries

To enable Intelligent CAM (iCAM) monitoring of ternary content addressable memory (TCAM) entries, use the **icam monitor entries** command. To disable the iCAM monitoring of TCAM entries, use the **no** form of this command.

```
icam monitor entries {acl module module inst instance | multicast module module}
```

```
no icam monitor entries {acl module module inst instance | multicast module module}
```

### Syntax Description

<b>acl</b>	Specifies the TCAM entries.
<b>module</b> <i>module</i>	Specifies the module number. The range is from 1–18 for an 18-slot chassis, and from 1–9 for a 9-slot chassis.
<b>inst</b> <i>instance</i>	Specifies the ASIC or forwarding engine instance number. The range is from 0–11.
<b>multicast</b>	Specifies the multicast entries.

### Command Default

iCAM monitoring of TCAM entries is not enabled. The historical traffic analytics and predictive analytics cannot be obtained for TCAM entries.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
Cisco NX-OS Release 8.2(1)	This command was introduced.

### Usage Guidelines

To use the **icam monitor entries** command, you must enable the iCAM feature using the **feature icam** command.

### Examples

This example shows how to enable iCAM monitoring on TCAM entries and multicast entries:

```
switch# configure terminal
switch(config)# icam monitor entries acl module 3 inst 0
switch(config)# icam monitor entries multicast module 3
```

This example shows how to disable iCAM monitoring on TCAM entries and multicast entries:

```
switch# configure terminal
switch(config)# no icam monitor entries acl module 3 inst 0
switch(config)# no icam monitor entries multicast module 3
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>feature icam</b>	Enables the iCAM feature.
	<b>icam monitor interval</b>	Configures the iCAM monitor interval and the number of intervals in an iCAM monitor history.
	<b>icam monitor resource</b>	Enables iCAM monitoring on TCAM resources.
	<b>show icam entries acl</b>	Displays traffic analytics of the ACL TCAM, which includes RACL, VACL, QoS, PBR, WCCP, CoPP, and so on.
	<b>show icam entries multicast</b>	Displays traffic analytics of multicast entries.
	<b>show icam prediction entries acl</b>	Displays machine-learning predictive analytics of the TCAM entries.
	<b>show icam prediction entries multicast</b>	Displays machine-learning predictive analytics of multicast entries.
	<b>show icam prediction resource</b>	Displays machine-learning predictive analytics of TCAM resource utilization.
	<b>show icam resource</b>	Displays TCAM resource utilization.

# icam monitor interval

To configure the Intelligent CAM (iCAM) monitor interval and the number of intervals in an iCAM monitor history, use the **icam monitor interval** command. To return the monitor interval and the number of intervals to their default values, use the **no** form of this command.

**icam monitor interval** *interval-hours* **num\_intervals** *num\_intervals*

**no icam monitor interval** *interval-hours* **num\_intervals** *num\_intervals*

## Syntax Description

<b>interval</b> <i>interval-hours</i>	Specifies the iCAM monitor interval, in hours. The range is from 1–12. The default is 1, and the interval duration is 7200 sec.
<b>num_intervals</b> <i>num_intervals</i>	Specifies the number of intervals in iCAM monitor history. The range is from 168–1344. The default is 168.

## Command Default

The iCAM feature uses the default values of the monitor interval and the number of intervals while monitoring the TCAM entries and resources to obtain traffic analytics.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco NX-OS Release 8.2(1)	This command was introduced.

## Usage Guidelines

To use the **icam monitor interval** command, you must enable the iCAM feature using the **feature icam** command.

## Examples

This example shows how to configure the iCAM monitoring interval and the number of intervals:

```
switch# configure terminal
switch(config)# icam monitor interval 2 num_intervals 200
```

This example shows how to reset the iCAM monitoring interval and the number of intervals:

```
switch# configure terminal
switch(config)# no icam monitor interval 2 num_intervals 200
```

## Related Commands

Command	Description
<b>feature icam</b>	Enables the iCAM feature.
<b>icam monitor entries</b>	Enables monitoring of the TCAM entries.
<b>icam monitor resource</b>	Enables monitoring of the TCAM resources.

<b>Command</b>	<b>Description</b>
<b>show icam entries acl</b>	Displays traffic analytics of the ACL TCAM, which includes RACL, VACL, QoS, PBR, WCCP, CoPP, and so on.
<b>show icam entries multicast</b>	Displays traffic analytics of multicast entries.
<b>show icam prediction entries acl</b>	Displays machine-learning predictive analytics of TCAM entries.
<b>show icam prediction entries multicast</b>	Displays machine-learning predictive analytics of multicast entries.
<b>show icam prediction resource</b>	Displays machine-learning predictive analytics of TCAM resource utilization.
<b>show icam resource</b>	Displays TCAM resource utilization.

## icam monitor resource

To enable Intelligent CAM (iCAM) monitoring on ternary content addressable memory (TCAM) resources, use the **icam monitor resource** command. To disable iCAM monitoring on TCAM resources, use the **no** form of this command.

**icam monitor resource** { **acl\_tcam** | **fib\_tcam** } **module** *module* **inst** *instance*

**no icam monitor resource** { **acl\_tcam** | **fib\_tcam** } **module** *module* **inst** *instance*

### Syntax Description

<b>acl_tcam</b>	Specifies the access control list (ACL) TCAM resources.
<b>module</b> <i>module</i>	Specifies the module number. The range is from 1–18 for an 18-slot chassis, and from 1–9 for a 9-slot chassis.
<b>inst</b> <i>instance</i>	Specifies the ASIC or forwarding engine instance number. The range is from 0–11.
<b>fib_tcam</b>	Specifies the forwarding information base (FIB) TCAM resources.

### Command Default

iCAM monitoring of TCAM resources are not enabled. The historical traffic analytics and predictive analytics cannot be obtained for TCAM resources.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
Cisco NX-OS Release 8.2(1)	This command was introduced.

### Usage Guidelines

To use the **icam monitor resource** command, you must enable the iCAM feature using the **feature icam** command.

### Examples

This example shows how to enable iCAM monitoring on ACL TCAM and FIB TCAM resources:

```
switch# configure terminal
switch(config)# icam monitor resource acl_tcam module 3 inst 0
switch(config)# icam monitor resource fib_tcam module 3 inst 0
```

This example shows how to disable iCAM monitoring on ACL TCAM and FIB TCAM resources:

```
switch# configure terminal
switch(config)# no icam monitor resource acl_tcam module 3 inst 0
switch(config)# no icam monitor resource fib_tcam module 3 inst 0
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>feature icam</b>	Enables the iCAM feature.
	<b>icam monitor entries</b>	Enables monitoring of TCAM entries.
	<b>icam monitor interval</b>	Configures the iCAM monitor interval and the number of intervals in an iCAM monitor history.
	<b>show icam entries acl</b>	Displays traffic analytics of the ACL TCAM, which includes RACL, VACL, QoS, PBR, WCCP, CoPP, and so on.
	<b>show icam entries multicast</b>	Displays traffic analytics of multicast entries.
	<b>show icam prediction entries acl</b>	Displays machine-learning predictive analytics of TCAM entries.
	<b>show icam prediction entries multicast</b>	Displays machine-learning predictive analytics of multicast entries.
	<b>show icam prediction resource</b>	Displays machine-learning predictive analytics of TCAM resource utilization.
	<b>show icam resource</b>	Displays TCAM resource utilization.

# ip access-list

To configure an IP access-list, use the **ip access-list** command.

**ip access-list** [*acl\_name* | **match-local-traffic**]

Syntax Description	
<i>acl_name</i>	Name of the access control list (ACL).
<b>match-local-traffic</b>	(Optional) Enables access-list matching for locally generated traffic.

Defaults	
None	

Command Modes	
config-acl	

Supported User Roles	
network-admin VDC-admin	

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

Usage Guidelines	
This command does not require a license.	

Examples	
This example shows how to configure an IP access list:	

```
switch# configure terminal
switch(config)# ip access-list match_12_pkts
switch(config-acl)# permit ip 12.0.0.0 0.255.255.255 any
switch(config-acl)#
```

Related Commands	Command	Description
	<b>filter access-group</b>	Applies an access control group to an Encapsulated Remote Switched Port Analyzer (ERSPAN) source session.



# ip dscp

To configure the differentiated devices code point (DSCP) value of the packets in the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic, use the **ip dscp** command.

**ip dscp** *dscp\_value*

<b>Syntax Description</b>	<i>dscp_value</i>	Value of the DSCP of the packets in the ERSPAN traffic. The range is from 0 to 63.
---------------------------	-------------------	--

<b>Defaults</b>	0
-----------------	---

<b>Command Modes</b>	config-erspan-src
----------------------	-------------------

<b>Supported User Roles</b>	network-admin network-operator
-----------------------------	-----------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.1(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to configure the DSCP value of the packets in the ESRSPAN traffic:

```
switch# configure terminal
switch(config)# monitor session 5 type erspan-source
switch(config-erspan-src)# ip dscp 10
switch(config-erspan-src)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip ttl</b>	Configures the IP time-to-live (TTL) value of the ERSPAN traffic.
	<b>monitor-session</b>	Enters the monitor configuration mode for configuring an ERSPAN or SPAN session for analyzing traffic between ports.

# ip flow monitor

To enable a Flexible NetFlow flow monitor for traffic that the router is receiving or forwarding, use the **ip flow monitor** command. To disable a Flexible NetFlow flow monitor, use the **no** form of this command.

```
ip flow monitor monitor-name {input | output} [sampler sampler-name]
```

Syntax Description		
	<i>monitor-name</i>	Name of a flow monitor that you previously configured.
	<b>input</b>	Monitors traffic that the routers are receiving on the interface.
	<b>output</b>	Monitors traffic that the routers are transmitting on the interface.
	<b>sampler</b>	(Optional) Specifies the name of a flow sampler for the flow monitor.
	<i>sampler-name</i>	Flow sampler for this flow monitor using the name of a sampler that you previously configured.

**Defaults** Disabled

**Command Modes** Interface configuration

**SupportedUserRoles** network-admin  
vdc-admin

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

**Usage Guidelines** You must have already created a flow monitor by using the **flow monitor** command before you can apply the flow monitor to an interface with the **ip flow monitor** command to enable traffic monitoring with Flexible NetFlow.

You must have already created a sampler by using the **sampler** command before you can enable a flow sampler for this flow monitor with the **ip flow monitor** command.

When adding a sampler to a flow monitor, only packets that are selected by the named sampler are entered into the cache to form flows. Each use of a sampler results in separate statistics being stored for that usage.

You cannot add a sampler to a flow monitor after the flow monitor has been enabled on an interface. You must remove the flow monitor from the interface before you enable the same flow monitor with a sampler. See the “Examples” section for more information.



**Note**

The statistics for each flow needs to be scaled to give the expected true usage. For example, if you are using a 1 in 10 sampler, you must multiply the packet and byte counters by 10.

This command does not require a license.

**Examples**

This example shows how to enable a flow monitor for monitoring input traffic:

```
switch(config)# vlan configuration 2
switch(config-vlan-config)# ip flow monitor FLOW-MONITOR-1 input
```



**Note**

- VLAN configuration mode enables you to configure VLANs independently of their creation, which is required for VTP client support.
- Egress NetFlow on VLAN is not supported

This example shows how to enable a flow monitor for monitoring output traffic:

```
switch(config)# interface ethernet0/0
switch(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

This example shows how to enable the same flow monitor on the same interface for monitoring input and output traffic:

```
switch(config)# interface ethernet0/0
switch(config-if)# ip flow monitor FLOW-MONITOR-1 input
switch(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

This example shows how to enable two different flow monitors on the same interface for monitoring input and output traffic:

```
switch(config)# interface ethernet0/0
switch(config-if)# ip flow monitor FLOW-MONITOR-1 input
switch(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

This example shows how to enable the same flow monitor on two different interfaces for monitoring input and output traffic:

```
switch(config)# interface ethernet0/0
switch(config-if)# ip flow monitor FLOW-MONITOR-1 input
switch(config)# interface ethernet1/0
switch(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

This example shows how to enable two different flow monitors on two different interfaces for monitoring input and output traffic:

```
switch(config)# interface ethernet0/0
switch(config-if)# ip flow monitor FLOW-MONITOR-1 input
switch(config)# interface ethernet1/0
switch(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

This example shows how to enable a flow monitor for monitoring input traffic with a sampler to limit the input packets that are sampled:

```
switch(config)# interface ethernet0/0
switch(config-if)# ip flow monitor FLOW-MONITOR-1 input sampler SAMPLER-1
```

This example shows how to enable a flow monitor for monitoring output traffic with a sampler to limit the output packets that are sampled:

```
switch(config)# interface ethernet0/0
switch(config-if)# ip flow monitor FLOW-MONITOR-1 output sampler SAMPLER-1
```

This example shows how to enable two different flow monitors for monitoring input and output traffic with a sampler on the flow monitor that is monitoring input traffic to limit the input packets that are sampled:

```
switch(config)# interface ethernet0/0
switch(config-if)# ip flow monitor FLOW-MONITOR-1 input sampler SAMPLER-1
switch(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

This example shows how to enable two different flow monitors for monitoring input and output traffic with a sampler on the flow monitor that is monitoring output traffic to limit the output packets that are sampled:

```
switch(config)# interface ethernet0/0
switch(config-if)# ip flow monitor FLOW-MONITOR-2 input
switch(config-if)# ip flow monitor FLOW-MONITOR-2 output sampler SAMPLER-1
```

This example shows what happens when you try to add a sampler to a flow monitor that has already been enabled on an interface without a sampler:

```
switch(config)# interface Ethernet0/0
switch(config-if)# ip flow monitor FLOW-MONITOR-1 input sampler SAMPLER-1
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

This example shows how to remove the flow monitor from the interface so that it can be enabled with the sampler:

```
switch(config)# interface Ethernet0/0
switch(config-if)# no ip flow monitor FLOW-MONITOR-1 input
switch(config-if)# ip flow monitor FLOW-MONITOR-1 input sampler SAMPLER-1
```

This example shows how to remove a sampler from a flow monitor on an interface by entering the **flow monitor** command again without the **sampler sampler-name** keyword and argument:

```
switch(config)# interface Ethernet0/0
switch(config-if)# ip flow monitor FLOW-MONITOR-1 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in sampled mode and cannot be
enabled in full mode.
```

This example shows how to remove the flow monitor that was enabled with a sampler from the interface so that it can be enabled without the sampler:

```
switch(config)# interface Ethernet0/0
switch(config-if)# no ip flow monitor FLOW-MONITOR-1 input sampler SAMPLER-1
switch(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

## Related Commands

Command	Description
<b>flow exporter</b>	Creates a flow exporter.
<b>flow monitor</b>	Creates a flow monitor.
<b>flow record</b>	Creates a flow record.
<b>sampler</b>	Creates a flow sampler.

# ip tftp source-interface

To configure source interface feature for TFTP client, use the **ip tftp source-interface** command. To disable this feature, use the **no** form of the command.

**ip tftp source-interface ethernet** *slot/chassis number* | **loopback** *virtual interface number*

**no ip tftp source-interface ethernet** *slot/chassis number* | **loopback** *virtual interface number*

Syntax Description		
<b>ethernet</b>		Specifies the ethernet IEEE 802.3z.
<i>slot/chassis number</i>		Specifies the slot or chassis number. The range is from 1 to 253.
<b>loopback</b>		Specifies the loopback interface.
<i>virtual interface number</i>		Specifies the virtual interface number. The range is from 0 to 1023.

**Defaults** None

**Command Modes** Global configuration mode

**Supported User Roles** network-admin  
VDC-admin

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

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

**Examples** This example shows how to configure the ethernet IEEE 802.3z:

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

This example shows how to configure the loopback interface:

```
switch(config)# ip tftp source-interface loopback 1
switch(config)#
```

**Related Commands**

Command	Description
<b>show ip tftp interface source-interface</b>	Displays source TFTP client information.

# ip ttl

To configure the IP time-to-live (TTL) value of the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic, use the **ip ttl** command.

**ip ttl** *ttl\_value*

<b>Syntax Description</b>	<i>ttl_value</i>	Value of the IP TTL of the ERSPAN traffic. The range is from 1 to 255.
---------------------------	------------------	--

<b>Defaults</b>	255
-----------------	-----

<b>Command Modes</b>	config-erspan-src and config-erspan-dst
----------------------	---

<b>Supported User Roles</b>	network-admin network-operator
-----------------------------	-----------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.1(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to configure the IP TTL value of the ESRSPAN source:

```
switch# configure terminal
switch(config)# monitor session 5 type erspan-source
switch(config-erspan-src)# ip ttl 30
switch(config-erspan-src)#
```

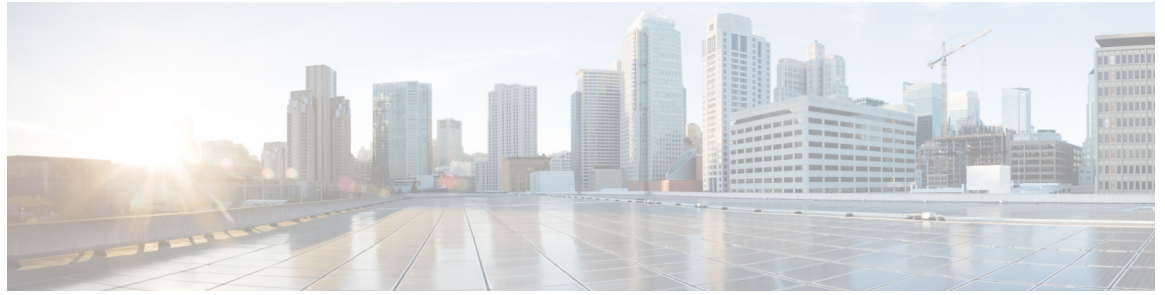
This example shows how to configure the IP TTL value of the ESRSPAN destination:

```
switch# configure terminal
switch(config)# monitor session 3 type erspan-destination
switch(config-erspan-dst)# ip ttl 35
switch(config-erspan-dst)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip dscp</b>	Configures the DSCP value of the packets in the ERSPAN traffic.
	<b>monitor-session</b>	Enters the monitor configuration mode for configuring an ERSPAN or SPAN session for analyzing traffic between ports.







# L Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter L.

# lldp holdtime

To configure the amount of time that a receiving device should hold the information sent by your device before discarding it, use the **lldp holdtime** command. To remove the hold time configuration, use the **no** form of this command.

**lldp holdtime** *seconds*

Syntax Description	<i>seconds</i>	Hold time in seconds. The range is from 10 to 255 seconds.
--------------------	----------------	--

Defaults	120 seconds
----------	-------------

Command Modes	Global configuration mode (config)
---------------	------------------------------------

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

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

Usage Guidelines	Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the <b>switchto vdc</b> command.
------------------	--

This command does not require a license.

Examples	This example shows how to configure the Link Layer Discovery Protocol (LLDP) hold time:
----------	---

```
switch(config)# lldp holdtime 180
switch(config)#
```

This example shows how to remove the LLDP hold time configuration:

```
switch(config)# no lldp holdtime 180
switch(config)#
```

Related Commands	Command	Description
	<b>lldp reinit</b>	Specifies the delay time in seconds for LLDP to initialize on any interface.

<b>Command</b>	<b>Description</b>
<b>lldp timer</b>	Specifies the transmission frequency of LLDP updates in seconds.
<b>show lldp timers</b>	Displays the LLDP holdtime, delay time, and update frequency configuration.

# lldp receive

To enable the reception of Link Layer Discovery Protocol (LLDP) packets on an interface, use the **lldp receive** command. To disable the reception of LLDP packets, use the **no** form of this command.

**lldp receive**

**no lldp receive**

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

**Defaults** None

**Command Modes** Interface configuration mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the **switchto vdc** command.

Make sure that you have globally enabled LLDP on the device.

This command does not require a license.

**Examples** This example shows how to enable the reception of LLDP packets on an interface:

```
switch(config)# interface ethernet 6/3
switch(config-if)# lldp receive
switch(config-if)# exit
switch(config)#
```

This example shows how to disable the reception of LLDP packets on an interface:

```
switch(config)# interface ethernet 6/3
switch(config-if)# no lldp receive
switch(config-if)# exit
switch(config)#
```

Related Commands	Command	Description
	lldp transmit	Enables the transmission of LLDP packets on an interface.
	show lldp interface ethernet	Displays the LLDP configuration on an interface.

# lldp reinit

To configure the delay time for the Link Layer Discovery Protocol (LLDP) to initialize on any interface, use the **lldp reinit** command. To remove the LLDP initialization configuration, use the **no** form of this command.

**lldp reinit** *seconds*

Syntax Description	<i>seconds</i>	Initialize time in seconds. The range is from 1 to 10.
--------------------	----------------	--

Defaults	2 seconds
----------	-----------

Command Modes	Global configuration mode (config)
---------------	------------------------------------

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

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

Usage Guidelines	Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the <b>switchto vdc</b> command.
------------------	--

This command does not require a license.

Examples	This example shows how to configure the delay time for LLDP initialization:
----------	---

```
switch(config)# lldp reinit 6
switch(config)#
```

This example shows how to remove the LLDP initialization configuration:

```
switch(config)# no lldp reinit 6
switch(config)#
```

Related Commands	Command	Description
	<b>lldp holdtime</b>	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.

<b>Command</b>	<b>Description</b>
<b>lldp timer</b>	Specifies the transmission frequency of LLDP updates in seconds.
<b>show lldp timers</b>	Displays the LLDP holdtime, delay time, and update frequency configuration.

# lldp timer

To configure the transmission frequency of Link Layer Discovery Protocol (LLDP) updates, use the **lldp timer** command. To remove the transmission frequency configuration for LLDP updates, use the **no** form of this command.

**lldp timer** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Transmission frequency in seconds. The range is from 5 to 254.
---------------------------	----------------	--

<b>Defaults</b>	30 seconds
-----------------	------------

<b>Command Modes</b>	Global configuration mode (config)
----------------------	------------------------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(1)	This command was introduced.

<b>Usage Guidelines</b>	Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the <b>switchto vdc</b> command.
-------------------------	--

This command does not require a license.

<b>Examples</b>	This example shows how to configure the transmission frequency for LLDP updates:
-----------------	--

```
switch(config)# lldp timer 45
switch(config)#
```

This example shows how to remove the transmission frequency configuration for LLDP updates:

```
switch(config)# no lldp timer 45
switch(config)#
```



**Related Commands**

<b>Command</b>	<b>Description</b>
<b>lldp reint</b>	Specifies the delay time in seconds for LLDP to initialize on any interface.
<b>lldp holdtime</b>	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.
<b>show lldp timers</b>	Displays the LLDP holdtime, delay time, and update frequency configuration.

# lldp tlv-select

To configure the type, length, and value (TLV) descriptions to send and receive in Link Layer Discovery Protocol (LLDP) packets, use the **lldp tlv-select** command. To remove the TLV configuration, use the **no** form of this command.

```
lldp tlv-select [dcbxp | management-address | port-description | port-vlan | system-capabilities
| system-description | system-name]
```

```
no lldp tlv-select [dcbxp | management-address | port-description | port-vlan |
system-capabilities | system-description | system-name]
```

## Syntax Description

<b>dcbxp</b>	(Optional) Specifies the DCBXP TLV.
<b>management-address</b>	(Optional) Specifies the Management Address TLV.
<b>port-description</b>	(Optional) Specifies the Port Description TLV.
<b>port-vlan</b>	(Optional) Specifies the Port VLAN ID TLV.
<b>system-capabilities</b>	(Optional) Specifies the System Capabilities TLV.
<b>system-description</b>	(Optional) Specifies the System Description TLV.
<b>system-name</b>	(Optional) Specifies the System Name TLV.

## Defaults

By default, all available TLVs are enabled.

## Command Modes

Global configuration mode (config)

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
5.0(1)	This command was introduced.

## Usage Guidelines

Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the **switchto vdc** command.

This command does not require a license.

---

**Examples**

This example shows how to enable the system capabilities TLV:

```
switch(config)# lldp tlv-select system-capabilities  
switch(config)#
```

This example shows how to disable the system capabilities TLV:

```
switch(config)# no lldp tlv-select system-capabilities  
switch(config)#
```

---

**Related Commands**

Command	Description
<b>show lldp tlv-select</b>	Displays the LLDP TLV configuration.
<b>show lldp dcbx</b> <b>interface ethernet</b>	Displays the local DCBX control status.

# lldp transmit

To enable the transmission of Link Layer Discovery Protocol (LLDP) packets on an interface, use the **lldp transmit** command. To disable the transmission of LLDP packets, use the **no** form of this command.

**lldp transmit**

**no lldp transmit**

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

**Defaults** Enabled

**Command Modes** Interface configuration mode

**Supported User Roles** network-admin  
vdc-admin

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

**Usage Guidelines** Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the **switchto vdc** command.

Make sure that you have globally enabled the LLDP on the device.

This command does not require a license.

**Examples** This example shows how to enable the transmission of LLDP packets on an interface:

```
switch(config)# interface ethernet 7/1
switch(config-if)# lldp transmit
switch(config-if)# exit
switch(config)#
```

This example shows how to disable the transmission of LLDP packets on an interface:

```
switch(config)# interface ethernet 7/1
switch(config-if)# no lldp transmit
switch(config-if)# exit
switch(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>lldp receive</b>	Enables the reception of LLDP packets on an interface.
	<b>show lldp interface ethernet</b>	Displays the LLDP configuration on an interface.

# locator-led

To blink an LED on the system, use the **locator-led** command. To restore the default LED state, use the **no** form of this command.

```
locator-led { chassis | fan f-number | module slot | powersupply ps-number | xbar x-number }
```

```
no locator-led { chassis | fan f-number | module slot | powersupply ps-number | xbar x-number }
```

## Syntax Description

<b>chassis</b>	Blinks the chassis LED.
<b>fan</b> <i>f-number</i>	Blinks the LED that represents the configured fan number. The range depends on the platform. Use ? to see the range.
<b>module</b> <i>slot</i>	Blinks the module LED. The range depends on the platform. Use ? to see the range.
<b>powersupply</b> <i>ps-number</i>	Blinks the power supply LED. The range depends on the platform. Use ? to see the range.
<b>xbar</b> <i>x-number</i>	Blinks the xbar module LED. The range depends on the platform. Use ? to see the range.

## Defaults

None

## Command Modes

Any command mode

## SupportedUserRoles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
4.1(2)	This command was introduced.

## Usage Guidelines

Use the **locator-led** command to flash the LED on a component in the system. You can use this blinking LED to identify the component to an administrator in the data center.

This command does not require a license.

## Examples

This example shows how to blink the LED for module 4:

```
switch# locator-led module 4
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show locator-led status</b>	Displays the status of locator LEDs on the system.

# 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

## Defaults

None

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## 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**

<b>Command</b>	<b>Description</b>
<b>show logging console</b>	Displays the console logging configuration.

# logging event

To log interface events, use the **logging event** command.

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

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

## Syntax Description

<b>link-status</b>	Logs all UP/DOWN and CHANGE messages.
<b>trunk-status</b>	Logs all TRUNK status messages.
<b>default</b>	Specifies that the default logging configuration is used by interfaces not explicitly configured.
<b>enable</b>	Specifies to enable logging to override the port level configuration.

## Defaults

None

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to log interface events:

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

## Related Commands

Command	Description
<b>show logging</b>	Displays the logging status.

# logging ip access-list cache

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

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

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

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

**Defaults** None

**Command Modes** Global configuration mode

**Supported User Roles** network-admin  
vdc-admin

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

**Usage Guidelines** This command does not require a license.  
Do not configure the cache threshold to a non-default value. Configure the cache interval to a lower value so that the syslog is generated from the cache entry expiry.

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

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

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

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

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

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

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show logging ip access-list</b>	Displays the status of IP access list logging.

---

# logging ip access-list detailed

To enable detailed logging, use the **logging ip access-list detailed** command in global configuration mode. To return to default, use the **no** form of this command.

**logging ip access-list detailed**

**no logging ip access-list detailed**

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

**Defaults** Detailed access list logging is disabled.

**Command Modes** Global configuration

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	6.2(6)	This command was introduced.

**Usage Guidelines** Access list logging information can be displayed to audit the data collected from the logged access-list entry. When detailed logging is enabled by using the **logging ip access-list detailed** command, the following additional parameters are collected along with the currently collected ACL-LOG fields:

- ACL Name
- ACE action (Permit/Deny)
- ACL Applied Interface (Appl Intr)

When detailed logging is enabled, the following additional parameters will be displayed in ACL-LOG cache entry along with the currently collected ACL-LOG fields:

- ACL Name
- ACE Number
- ACE Action (Permit /Deny)
- ACL Direction (Ingress/Egress)
- ACL Filter Type (RACL\_IPV4/PACL\_MAC/ PACL\_IPV4/PBR/VACL)
- ACL Applied Interface

This command does not require a license.

---

**Examples**

This example shows how to configure detailed access list logging:

```
switch# config t  
switch(config)# logging ip access-list detailed
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show logging ip access-list cache</b>	Displays information about the IP access list logging cache.

# logging level

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

**logging level** *facility severity-level*

**no logging level** *facility severity-level*

<b>Syntax Description</b>	<i>facility</i>	Appropriate <i>facility</i> . The facilities are listed in the <a href="#">“System Message Logging Facilities”</a> section on page 1.
		To apply the same severity level to all facilities, use the <b>all</b> 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"> <li>• <b>0</b>—emergency: System unusable</li> <li>• <b>1</b>—alert: Immediate action needed</li> <li>• <b>2</b>—critical: Critical condition—default level</li> <li>• <b>3</b>—error: Error condition</li> <li>• <b>4</b>—warning: Warning condition</li> <li>• <b>5</b>—notification: Normal but significant condition</li> <li>• <b>6</b>—informational: Informational message only</li> <li>• <b>7</b>—debugging: Appears during debugging only</li> </ul>
<b>Defaults</b>	None	
<b>Command Modes</b>	Global configuration mode	
<b>SupportedUserRoles</b>	network-admin vdc-admin	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.
<b>Usage Guidelines</b>	This command does not require a license.	

---

**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)#
```

---

**Related Commands**

Command	Description
<b>show logging level</b>	Displays the facility logging level configuration.



# 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"> <li>• <b>0</b>—emergency: System unusable</li> <li>• <b>1</b>—alert: Immediate action needed</li> <li>• <b>2</b>—critical: Critical condition—default level</li> <li>• <b>3</b>—error: Error condition</li> <li>• <b>4</b>—warning: Warning condition</li> <li>• <b>5</b>—notification: Normal but significant condition</li> <li>• <b>6</b>—informational: Informational message only</li> <li>• <b>7</b>—debugging: Appears during debugging only</li> </ul>
<i>size bytes</i>	(Optional) Specifies a maximum file size. The default file size is 10485760 bytes and can be configured from 4096 to 10485760 bytes.

**Defaults** None

**Command Modes** Global configuration mode

**SupportedUserRoles** network-admin  
vdc-admin

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

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

---

**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)#
```

---

**Related Commands**

Command	Description
<b>show logging logfile</b>	Displays the log file.

# logging message interface type ethernet description

To add the description for physical Ethernet interfaces and subinterfaces in the system message log, use the **logging message interface type ethernet description** command. To disable the printing of the interface description for physical Ethernet interfaces in the system message log, use the **no** form of this command.

**logging message interface type ethernet description**

**no logging message interface type ethernet description**

**Syntax Description** This command does not have any arguments or password.

**Defaults** None

**Command Modes** Global configuration mode

**SupportedUserRoles** network-admin  
vdc-admin

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

**Usage Guidelines** Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command. This command does not require a license.

**Examples** This example shows how to add the description for physical Ethernet interfaces and subinterfaces in the system message log:

```
switch# configure terminal
switch(config)# logging message interface type ethernet description
```

## ■ logging message interface type ethernet description

This example shows how to disable the printing of the interface description for physical Ethernet interfaces in the system message log:

```
switch# configure terminal  
switch(config)# no logging message interface type ethernet description
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>logging monitor</b>	Enables the device to log messages to the monitor based on a specified severity level or higher.
<b>show logging monitor</b>	Displays the monitor logging configuration.

# 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**

<b>Syntax Description</b>	<p><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:</p> <ul style="list-style-type: none"> <li>• <b>0</b>—emergency: System unusable</li> <li>• <b>1</b>—alert: Immediate action needed</li> <li>• <b>2</b>—critical: Critical condition</li> <li>• <b>3</b>—error: Error condition</li> <li>• <b>4</b>—warning: Warning condition</li> <li>• <b>5</b>—notification: Normal but significant condition—default level</li> <li>• <b>6</b>—informational: Informational message only</li> <li>• <b>7</b>—debugging: Appears during debugging only</li> </ul>				
<b>Defaults</b>	None				
<b>Command Modes</b>	Global configuration mode				
<b>SupportedUserRoles</b>	network-admin vdc-admin				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
<b>Usage Guidelines</b>	This command does not require a license.				
<b>Examples</b>	<p>This example shows how to enable module log messages:</p> <pre>switch# <b>configure terminal</b> switch(config)# <b>logging module</b> switch(config)#</pre>				

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show logging module</b>	Displays the module logging status.

# logging monitor

To log messages to the monitor (terminal line), use the **logging monitor** command to enable the device.

To disable monitor log messages, use the **no** form of this command.

**logging monitor** [*severity-level*]

**no logging monitor**

## 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"> <li>• <b>0</b>—emergency: System unusable</li> <li>• <b>1</b>—alert: Immediate action needed</li> <li>• <b>2</b>—critical: Critical condition—default level</li> <li>• <b>3</b>—error: Error condition</li> <li>• <b>4</b>—warning: Warning condition</li> <li>• <b>5</b>—notification: Normal but significant condition</li> <li>• <b>6</b>—informational: Informational message only</li> <li>• <b>7</b>—debugging: Appears during debugging only</li> </ul>
-----------------------	---

## Defaults

5

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This configuration applies to Telnet and SSH sessions.

This command does not require a license.

---

**Examples**

This example shows how to enable monitor log messages:

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

---

**Related Commands**

Command	Description
<b>show logging monitor</b>	Displays the status of monitor logging.



# 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 [use-vrf VRF_name [facility {auth | authpriv | cron | daemon
| ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news
| syslog | user | uucp}]]]
```

```
no logging server host
```

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"> <li>• <b>0</b>—emergency: System unusable</li> <li>• <b>1</b>—alert: Immediate action needed</li> <li>• <b>2</b>—critical: Critical condition—default level</li> <li>• <b>3</b>—error: Error condition</li> <li>• <b>4</b>—warning: Warning condition</li> <li>• <b>5</b>—notification: Normal but significant condition</li> <li>• <b>6</b>—informational: Informational message only</li> <li>• <b>7</b>—debugging: Appears during debugging only</li> </ul>
<b>use-vrf</b> <i>VRF_name</i>	(Optional) Specifies the VPN routing and forwarding (VRF) instance. In Cisco NX-OS Release 4.2 or later releases, the default VRF is default.
<b>facility</b> <i>facility</i>	(Optional) Specifies the outgoing <i>facility</i> . The facilities are listed in the “ <a href="#">System Message Logging Facilities</a> ” section on page 1. The default outgoing facility is <b>local7</b> .

**Defaults** None

**Command Modes** Global configuration mode

**Supported User Roles** network-admin  
vdc-admin

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

---

**Usage Guidelines**

This command does not require a license.

---

**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 172.28.254.253
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**

---

<b>Command</b>	<b>Description</b>
<b>show logging server</b>	Displays the configured syslog servers.

---

# logging source-interface

To enable a source interface whose IP address is displayed in all the log messages, use the **logging source-interface** command.

To disable the source interface, use the **no** form of this command.

**logging source-interface** *interface*

**no logging source-interface** *interface*

<b>Syntax Description</b>	<i>interface</i>	The interface whose IP address is displayed in all the log messages.
<b>Defaults</b>	None	
<b>Command Modes</b>	Global configuration.	
<b>SupportedUserRoles</b>	network-admin vdc-admin	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.
	7.3(0)N1(1)	This command was modified to ensure that the same IP address appears in all messages sent from an individual Cisco NX-OS device.
<b>Usage Guidelines</b>	This command does not require a license.	
<b>Examples</b>	<p>This example shows how to specify that the IP address of the loopback 5 interface should be used for all log messages:</p> <pre>switch# <b>configure terminal</b> switch(config)# <b>logging source-interface loopback 5</b> switch(config)#</pre>	

# logging timestamp

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

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

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

## Syntax Description

<b>microseconds</b>	Specifies the time stamp unit in microseconds. The default units are <b>seconds</b> .
<b>milliseconds</b>	Specifies the time stamp unit in milliseconds.
<b>seconds</b>	Specifies the time stamp unit in seconds.

## Defaults

None

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

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

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

## Related Commands

Command	Description
<b>show logging timestamp</b>	Displays the logging time stamp configuration.



# M Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter M.

# match datalink

To configure the match data link (or Layer 2) attributes option in a flow record, use the **match datalink** command. To remove the data link configuration, use the **no** form of this command.

```
match datalink { mac source-address | mac destination-address | ethertype | vlan }
```

```
no match datalink { mac source-address | mac destination-address | ethertype | vlan }
```

## Syntax Description

<b>mac</b>	Specifies the MAC address.
<b>source-address</b>	Specifies the source MAC address.
<b>destination-address</b>	Specifies the destination MAC address.
<b>ethertype</b>	Specifies the EtherType.
<b>vlan</b>	Specifies the VLAN ID.

## Defaults

None

## Command Modes

NetFlow record configuration (config-flow-record)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.1	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure the match data link attributes option in a flow record:

```
switch(config)# flow record NetFlow1
switch(config-flow-record)# match datalink mac source-address
switch(config-flow-record)#
```

This example shows how to remove the data link match option from a flow record:

```
switch(config-flow-record)# no match datalink mac source-address
switch(config-flow-record)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>match ip</b>	Configures the match IP option for defining a NetFlow record map.
<b>match ipv4</b>	Configures the match IPv4 option for defining a NetFlow record map.

# match ip

To configure the match IP option for defining a NetFlow record map, use the **match ip** command. To remove this option, use the **no** form of this command.

```
match ip {protocol | tos}
```

```
no match ip {protocol | tos}
```

## Syntax Description

<b>protocol</b>	Specifies the protocol.
<b>tos</b>	Specifies the type of service (ToS).

## Defaults

None

## Command Modes

NetFlow record configuration (config-flow-record)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure the match IP option for defining a NetFlow record map:

```
switch(config)# flow record Custom-NetFlow-Record-1
switch(config-flow-record)# match ip protocol
switch(config-flow-record)# match ip tos
switch(config-flow-record)#
```

This example shows how to remove the match option:

```
switch(config-flow-record)# no match ip protocol
switch(config-flow-record)# no match ip tos
switch(config-flow-record)#
```

## Related Commands

Command	Description
<b>show flow record</b>	Displays information about NetFlow records.



# match ipv4

To configure the match IPv4 option for defining a NetFlow record map, use the **match ipv4** command. To remove this option, use the **no** form of this command.

```
match ipv4 {source | destination} address
```

```
no match ipv4 {source | destination} address
```

## Syntax Description

<b>source</b>	Specifies the source address.
<b>destination</b>	Specifies the destination address.
<b>address</b>	Specifies the address.

## Defaults

None

## Command Modes

NetFlow record configuration (config-flow-record)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure the match IPv4 option for defining a NetFlow record map:

```
switch(config)# flow record Custom-NetFlow-Record-1
switch(config-flow-record)# match ipv4 source address
switch(config-flow-record)# match ipv4 destination address
switch(config-flow-record)#
```

This example shows how to remove the match IPv4 configuration:

```
switch(config-flow-record)# no match ipv4 source address
switch(config-flow-record)# no match ipv4 destination address
switch(config-flow-record)#
```

## Related Commands

Command	Description
<b>show flow record</b>	Displays information about NetFlow records.

# match (NetFlow)

To specify match criteria for Flexible NetFlow flow records, use the **match** command. To remove match criteria for flow records, use the **no** form of this command.

```
match { flow direction | interface { input | output } | ip { protocol | tos } | ipv4 { destination address
| source address } | transport { destination-port | source-port } }
```

```
match { flow direction | interface { input | output } | ip { protocol | tos } | ipv4 { destination address
| source address } | transport { destination-port | source-port } }
```

## Syntax Description

<b>flow direction</b>	Specifies the direction of the flow to be matched.
<b>interface input</b>	Specifies that the match criterion is based on the input interface.
<b>interface output</b>	Specifies that the match criterion is based on the output interface.
<b>ip protocol</b>	Specifies that the match criterion is based on protocol.
<b>ip tos</b>	Specifies that the match criterion is based on type of service (ToS).
<b>ipv4 destination address</b>	Specifies that the match criterion is based on the destination IPv4 address.
<b>ipv4 source address</b>	Specifies that the match criterion is based on the source IPv4 address.
<b>transport destination-port</b>	Specifies that the match criterion for transport layer fields is based on the destination port.
<b>transport source-port</b>	Specifies that the match criterion for transport layer fields is based on the destination port.

## Defaults

No matching criteria are specified by default.

## Command Modes

Flow record configuration

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

A Flexible NetFlow flow record must be enabled before you can use the **match** command.

To export Layer 4 data, you must configure both the **match transport** and the **match ip protocol** commands. The data is collected and displayed in the output of the **show hardware flow ip** command but is not collected and exported until you configure both commands.

This command does not require a license.

## Examples

This example shows how to specify the direction of the flow to be matched:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match flow direction
```

This example shows how to specify the match criterion is based on the input interface:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match interface input
```

This example shows how to specify that the match criterion is based on the output interface:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match interface output
```

This example shows how to specify that the match criterion is based on protocol:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match ip protocol
```

This example shows how to specify that the match criterion is based on type of service (ToS):

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match ip tos
```

This example shows how to specify that the match criterion is based on the destination IPv4 address:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match ipv4 destination address
```

This example shows how to specify that the match criterion is based on the source IPv4 address:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match ipv4 source address
```

This example shows how to specify that the match criterion for transport layer fields is based on the destination port:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match ipv4 transport destination-port
```

This example shows how to specify that the match criterion for transport layer fields is based on the source port:

```
switch(config)# flow record FLOW-RECORD-1
switch(config-flow-record)# match ipv4 transport source-port
```

## Related Commands

Command	Description
<b>flow record</b>	Creates a flow record.

# match transport

To configure the match transport option for defining a NetFlow record map, use the **match transport** command. To remove the match transport option, use the **no** form of this command.

```
match transport { destination-port | source-port }
```

```
no match transport { destination-port | source-port }
```

## Syntax Description

**destination-port** Specifies the transport destination port.

**source-port** Specifies the transport source port.

## Defaults

None

## Command Modes

NetFlow record configuration (config-flow-record)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure the match transport option for defining a NetFlow record map:

```
switch(config)# flow record Custom-NetFlow-Record-1  
switch(config-flow-record)# match transport source-port
```

This example shows how to remove the configuration:

```
switch(config-flow-record)# no match transport source-port  
switch(config-flow-record)
```

## Related Commands

Command	Description
<b>show flow record</b>	Displays information about NetFlow records.

# mode

To specify the mode in a NetFlow sampler, use the **mode** command. To remove the mode, use the **no** form of this command.

**mode** *samples*

**no mode** [*samples*]

Syntax Description	<i>samples</i>	Number of samples per sampling. The range is from 1 to 64.
--------------------	----------------	--

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

Command Modes	NetFlow sampler configuration (config-flow-sampler)
---------------	---

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

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

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



### Note

For F2 Series modules, an additional sampling of 1:100 is applied over the configured value. For example, if the configured sampling is 1 in 800, the actual applied sampling is 1 in 80000. With this always-enabled additional 1:100 sampling, the packets range for all F2 Series module ports is from 1 to 819100.

Examples	This example shows how to specify the mode in a NetFlow sampler:
----------	--

```
switch(config)# sampler Custom-NetFlow-Sampler-1
switch(config-flow-sampler)# mode 1 out-of 1000
switch(config-flow-sampler)#
```

This example shows how to remove the mode configuration:

```
switch(config-flow-sampler)# no mode
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show sampler</b>	Displays information about NetFlow samplers.

# mode extended

To configure the Ethernet Switched Port Analyzer (SPAN) session as an extended bidirectional session, use the **mode extended** command. To remove the SPAN session as an extended bidirectional session, use the **no** form of this command.

**mode extended**

**no mode extended**

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

**Defaults** None

**Command Modes** Monitor configuration mode (config-monitor)

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	6.2(2)	This command was introduced.

**Usage Guidelines** You cannot use this command for a unidirectional SPAN session.

Extended SPAN sessions cannot source incoming traffic on M1 Series modules in either the ingress or egress direction. Extended SPAN sessions support traffic only from the F Series and M2 Series modules.

Hardware session 15 is used by NetFlow on F2 and F2e Series modules. Any extended session using this hardware ID will not span incoming traffic on the F2 and the F2e ports.

This command does not require a license.

**Examples** This example shows how to configure the SPAN session as an extended bidirectional session:

```
switch(config)# monitor session 3 tx
switch(config-monitor)# mode extended
```

Related Commands	Command	Description
	<b>monitor session</b>	Places you in the monitor configuration mode for configuring a SPAN session.

# monitor counter

To configure a Simple Network Management Protocol (SNMP) monitor counter, use the **monitor counter** command. To remove a monitor counter configuration, use the **no** form of this command.

```
monitor counter { invalid-crc | invalid-words | link-loss | protocol-error | rx-performance |
signal-loss | state-change | sync-loss | tx-performance }
```

```
no monitor counter { invalid-crc | invalid-words | link-loss | protocol-error | rx-performance |
signal-loss | state-change | sync-loss | tx-performance }
```

## Syntax Description

<b>invalid-crc</b>	Configures the invalid-crc counter.
<b>invalid-words</b>	Configures the invalid-words counter.
<b>link-loss</b>	Configures the link-loss counter.
<b>protocol-error</b>	Configures the protocol-error counter.
<b>rx-performance</b>	Configure the ingress (rx) performance counter.
<b>signal-loss</b>	Configures the signal-loss counter.
<b>state-change</b>	Configures the state-change counter.
<b>sync-loss</b>	Configures the sync-loss counter.
<b>tx-performance</b>	Configures the egress (tx) performance counter.

## Defaults

None

## Command Modes

Port-monitor configuration (config-port-monitor)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.1(2)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure an SNMP counter:

```
switch(config) port-monitor name PM1
switch(config-port-monitor) # monitor counter signal-loss
switch(config-port-monitor) #
```

This example shows how to remove a counter configuration:



```
switch(config)# no monitor counter signal-loss  
switch(config-port-monitor)#
```

**Related Commands**

Command	Description
<b>counter</b>	Configures an individual counter.

# monitor erspan origin ip-address

To configure the Encapsulated Remote Switched Port Analyzer (ERSPAN) origin IP address, use the **monitor erspan origin ip-address** command. To remove the ERSPAN 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**

<b>Syntax Description</b>	<i>ip-address</i>	Global origin IP address.
	<b>global</b>	(Optional) Specifies the default virtual device context (VDC) configuration across all VDCs.

**Defaults** None

**Command Modes** Global configuration mode (config)

**Supported User Roles** network-admin  
vdc-admin

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.1(1)	This command was introduced.

**Usage Guidelines** The global origin IP address can be configured in either the default VDC or the admin VDC. The value that is configured in this VDC is valid across all VDCs.

When you change the origin IP address in the default VDC, it impacts all of the sessions.

This command does not require a license.

**Examples** This example shows how to configure the ERSPAN 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 IP address:

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

# monitor erspan granularity

To configure the granularity for Encapsulated Remote Switched Port Analyzer (ERSPAN) Type III sessions, use the **monitor erspan granularity** command. To remove this feature, use the **no** form of this command.

```
monitor erspan granularity { 100_ms | 100_ns | 1588 | ns }
```

```
no monitor erspan granularity { 100_ms | 100_ns | 1588 | ns }
```

## Syntax Description

<b>100_ms</b>	Specifies 100 microseconds.
<b>100_ns</b>	Specifies 100 nanoseconds.
<b>1588</b>	Specifies the IEEE 1588 time representation format in seconds or nanoseconds.
<b>ns</b>	Specifies nanoseconds.

## Defaults

vdc

## Command Modes

Global configuration mode (config)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
6.1(1)	This command was introduced.

## Usage Guidelines

The clock manager adjusts the ERSPAN timers based on the granularity setting. If you configure IEEE 1588, the clock manager synchronizes the ERSPAN timers across switches. Otherwise, the clock manager synchronizes the ERSPAN timer with the master timer in the switch.

588 granularity mode is not supported in Cisco NX-OS Release 6.1 and is rejected if selected.

M2 Series modules support 100 microseconds, 100 nanoseconds, and nanoseconds granularity. F2 Series and F2e Series modules support only 100 microseconds and 100 nanoseconds granularity.

This command can be applied only in the default VDC.

This command does not require a license.

## Examples

This example shows how to configure the granularity for 100 microseconds:

```
switch# configure terminal
switch(config)# monitor erspan granularity 100_ms
switch(config)#
```

# monitor session

To enter the monitor configuration mode for configuring Encapsulated Remote Switched Port Analyzer (ERSPAN) or an Ethernet Switched Port Analyzer (SPAN) session for analyzing traffic between ports, use the **monitor session** command. To disable an ERSPAN or an SPAN session(s), use the **no** form of this command.

```
monitor session { session_number | all } { rx | tx | type [erspan-source | erspan-destination | local] | shut }
```

```
no monitor session { session_number | all } [shut]
```

## Syntax Description

<i>session_number</i>	Session number to use for monitoring a switched port. The range is from 1 to 48.
<b>all</b>	Specifies all sessions for monitoring a switched port.
<b>rx</b>	Specifies an ingress-extended SPAN session.
<b>tx</b>	Specifies an egress-extended SPAN session.
<b>type</b>	Specifies a session type. A session type can be <b>local</b> , <b>erspan-source</b> , or <b>erspan-destination</b> .
<b>erspan-source</b>	(Optional) Creates an ERSPAN source session.
<b>erspan-destination</b>	(Optional) Creates an ERSPAN destination session.
<b>local</b>	(Optional) Creates a local session.
<b>shut</b>	Specifies a shut state for the selected session.

## Defaults

None

## Command Modes

Global configuration mode (config)

## Supported User Roles

Super user  
VDC administrator  
VDC user

## Command History

Release	Modification
6.2(2)	Added the <b>rx</b> , <b>tx</b> , and <b>shut</b> keywords.
5.1(1)	The number of sessions has been increased to 48.
4.0(1)	This command was introduced.

## Usage Guidelines

While configuring an ERSPAN source session, if **rx**, **tx**, or both keywords are not entered, the source is configured for both directions.

The new session configuration is added to the existing session configuration. By default, the session is created in the shut state, and the session is a local SPAN session.

For more information about the ERSPAN configuration, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*.

This command does not require a license.

## Examples

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

```
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 shut
```

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

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

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

```
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
```

This example shows how to terminate or extend RSPAN:

```
switch(config)# vlan 200
switch(config-vlan)# remote-span
switch(config-vlan)#
```

This example shows how to monitor RSPAN VLAN traffic using a local SPAN:

```
switch(config)# monitor session 1 type local
switch(config-monitor)# description RSPAN VLAN as source
switch(config-monitor)# source vlan 200
switch(config-monitor)# destination interface ethernet 1/2
switch(config-monitor)# no shut
switch(config-monitor)#
```

This example shows how to disable a SPAN session:

```
switch(config)# no monitor session 9 type local
```

This example show how to create an ERSPAN source:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-monitor-erspan-src)# source int eth1/1
switch(config-monitor-erspan-src)# destination ip address 10.1.1.1
switch(config-monitor-erspan-src)# erspan-id 101
switch(config-monitor-erspan-src)# vrf erspan-vrf
switch(config-monitor-erspan-src)# filter vlan 100
switch(config-monitor-erspan-src)# no shut
```

This example show how to create an ERSPAN destination:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-destination
switch(config-monitor-erspan-dst)# destination interface eth1/5
switch(config-monitor-erspan-dst)# vrf foo
switch(config-monitor-erspan-dst)# erspan-id 12
switch(config-monitor-erspan-dst)# source ip 10.1.1.1
switch(config-monitor-erspan-dst)# no shut
```

This example show how to create an access control list (ACL) filter and associate it with the ERSPAN source, IP time-to-leave (TTL), and differentiated services code point (DSCP) value:

```
switch# configure terminal
switch(config)# monitor session 3 type erspan-source
switch(config-monitor)# description erspan_src_session_3
switch(config-monitor-erspan-src)# source interface port-channel 2
switch(config-monitor-erspan-src)# filter vlan 3-5, 7
switch(config-monitor-erspan-src)# filter access-group ACL1
switch(config-monitor-erspan-src)# destination ip-address 10.1.1.1
switch(config-monitor-erspan-src)# erspan-id 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# ip ttl 25
switch(config-erspan-src)# ip dscp 42
switch(config-monitor-erspan-src)# exit
```

#### Related Commands

Command	Description
<b>show monitor session</b>	Displays the specified SPAN or ERSPAN session configuration.
<b>description</b>	Adds a comment or a description of up to 32 characters to a SPAN session.
<b>destination</b>	Adds a SPAN destination where source packets are copied.
<b>source</b>	Configures the source and the traffic direction in which to copy packets for a SPAN and ERSPAN session.

# mtu

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

**mtu** *mtu-size*

**no mtu**

## Syntax Description

<i>mtu-size</i>	MTU truncation size. The configurable range is from 176 to 1500 bytes. The local SPAN range is from 64 to 1500 bytes.
-----------------	---

## Defaults

Disabled

## Command Modes

Monitor configuration (config-monitor)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
6.1(1)	Starting with 6.1, MTU truncation also support ERSPAN session.
5.2(1)	This command was introduced.

## Usage Guidelines

Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.

MTU truncation and the SPAN rate limit cannot be enabled for the same SPAN session. If you configure both for one session, only the rate limit is allowed on F1 Series modules, and MTU truncation is disabled until you disable the rate limit configuration. This limitation does not apply to F2 and M2 Series modules or Supervisor 2.

MTU truncation and the ERSPAN source rate limit are supported only on F Series and M2 Series modules and Supervisor 2. They are not supported on M1 Series modules.



### Note

MTU truncation and ERSPAN sampling can be enabled at the same time and have no precedence over each other because they are applied to different aspects of the source packet (size versus packet count).

This command does not require a license.

## Examples

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

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

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

```
switch# configure terminal
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# mtu 100
```

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

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

## Related Commands

Command	Description
<b>monitor session</b>	Places you in the monitor configuration mode for configuring a SPAN session.
<b>show monitor session</b>	Displays the status of the SPAN or ERSPAN session.



# multicast best-effort

To configure the multicast best effort mode for the specified Encapsulated Remote Switched Port Analyzer (ERSPAN) or the Ethernet Switched Port Analyzer (SPAN) session, use the **multicast best-effort** command. To remove the multicast best effort mode for an ERSPAN or SPAN session, use the **no** form of this command.

**multicast best-effort**

**no multicast best-effort**

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

**Defaults** Disabled

**Command Modes** Monitor configuration (config-monitor)

**SupportedUserRoles** network-admin  
vdc-admin

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

**Usage Guidelines** By default, SPAN replication occurs on both the ingress and egress line card. When you enable the multicast best effort mode, SPAN replication occurs only on the ingress line card for multicast traffic or on the egress line card for packets egressing out of Layer 3 interfaces (that is, on the egress line card, packets egressing out of Layer 2 interfaces are not replicated for SPAN).

Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.



**Note** Multicast best effort mode applies only to M1 Series modules

This command does not require a license.

**Examples** This example shows how to configure the multicast best effort mode for the specifies ERSPAN or SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# multicast best-effort
switch(config-monitor)#
```

This example shows how to remove the multicast best effort mode for the specified ERSPAN or SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# no multicast best-effort
switch(config-monitor)#
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>monitor session</b>	Places you in the monitor configuration mode for configuring a SPAN session.
<b>show monitor session</b>	Displays the status of the SPAN or ERSPAN session.

---



# N Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter N.

# ntp abort

To abort the Network Time Protocol (NTP) configuration, use the **ntp abort** command.

**ntp abort**

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

**Defaults** None

**Command Modes** Global configuration mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

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

```
switch# ntp abort
No changes to abort
switch#
```

Related Commands	Command	Description
	<b>ntp commit</b>	Commits the NTP configuration.
	<b>ntp distribute</b>	Enables Cisco Fabric Services (CFS) distribution for NTP.

# 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 | match-all} access-list-name
```

```
no ntp access-group {peer | serve | serve-only | query-only | match-all} access-list-name
```

## Syntax Description

<b>peer</b>	Allows the device to receive time requests and NTP control queries to synchronize itself to the servers specified in the access list.
<b>serve</b>	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.
<b>serve-only</b>	Allows the device to receive only time requests from servers specified in the access list.
<b>query-only</b>	Allows the device to receive only NTP control queries from the servers specified in the access list.
<b>match-all</b>	Enables the access group options to be scanned in the following order: peer, serve, serve-only, query-only.
<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

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
6.2(2)	Added the <b>match-all</b> keyword.
5.2(1)	Added the <b>serve</b> , <b>serve-only</b> , and <b>query-only</b> keywords.
5.0(1)	This command was introduced.

## Usage Guidelines

Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.

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.

The **ntp access-group match-all** command is available beginning with Cisco NX-OS Release 6.2(2). If you enter the **no** form of this command, do not enter this command or create an access group using an earlier version of Cisco NX-OS. ACL processing stops and does not continue to the next access group option if the incoming packet does not match the peer access group or if NTP matches a deny ACL rule in a configured peer.

This command does not require a license.

### Examples

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

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

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

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

### Related Commands

Command	Description
<b>feature ntp</b>	Enables the NTP on a VDC.
<b>show ntp access-groups</b>	Displays the NTP access groups.

# ntp authenticate

To prevent the system from synchronizing with unauthenticated, unconfigured network peers, use the **ntp authenticate** command. Use the **no** form of this command to allow synchronization with unauthenticated, unconfirmed network peers.

**ntp authenticate**

**no ntp authenticate**

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

**Command Default** Disabled

**Command Modes** Global configuration mode (config)

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** If the system has been configured with the **ntp passive**, **ntp broadcast client**, or **ntp multicast client** commands, when NTP receives an incoming symmetric active, broadcast, or multicast packet, it can set up an ephemeral peer association in order to synchronize with the sender.

If **ntp authenticate** is specified, when a symmetric active, broadcast, or multicast packet is received, the system will not synchronize to the peer unless the packet carries one of the authentication keys specified in the **ntp trusted-key** global configuration command.

To prevent synchronization with unauthorized network hosts, **ntp authenticate** should be specified any time **ntp passive**, **ntp broadcast client**, or **ntp multicast client** has been specified unless other measures, such as the **ntp access-group** command, have been taken to prevent unauthorized hosts from communicating with the NTP service on the device.

Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.

This command does not require a license.



**Note** This command does not authenticate peer associations configured via the **ntp server** and **ntp peer** commands. To authenticate ntp server and ntp peer associations, specify the **key** keyword.

### Examples

This example shows how to enable NTP authentication:

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

This example shows how to disable NTP authentication:

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

### Related Commands

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



# 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 md5 md5-string*

**no ntp authentication-key** *number md5 md5-string*

Syntax Description		
	<i>number</i>	Authentication key number. The range is from 1 to 65535.
	<b>md5</b>	Specifies the MD5 algorithm for authentication.
	<i>md5-string</i>	MD5 string. Cisco NX-OS Release 5.2(3) and later 5.x releases support up to 15 alphanumeric characters for the MD5 string. Earlier 5.x releases and Cisco NX-OS Release 6.0(1) support up to 8 alphanumeric characters.

**Defaults** Disabled

**Command Modes** Global configuration mode (config)

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	5.2(3)	Increases the length of NTP authentication keys from 8 to 15 alphanumeric characters.
	5.0(1)	This command was introduced.

**Usage Guidelines** Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.

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.

This command does not require a license.

---

**Examples**

This example shows how to configure an NTP authentication key:

```
switch# config t  
switch(config)# ntp authentication-key 42 md5 aNiceKey  
switch(config)#
```

This example shows how to remove the NTP authentication key:

```
switch# config t  
switch(config)# no ntp authentication-key 42 md5 aNiceKey  
switch(config)#
```

---

**Related Commands**

Command	Description
<b>show ntp authentication-key</b>	Configures one or more keys that a time source must provide in its NTP packets in order for the device to synchronize to it.

# 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

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

## Defaults

None

## Command Modes

Interface configuration mode (config-if)

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
6.2(2)	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
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ntp enable</b>	Enables NTP.

# 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*]

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

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Global configuration mode
----------------------	---------------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

Command History	Release	Modification
	6.2(2)	This command was introduced.

<b>Usage Guidelines</b>	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.

<b>Examples</b>	This example shows how to configure the estimated broadcast round-trip delay:
-----------------	---

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

■ ntp broadcastdelay

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ntp enable</b>	Enables NTP.

# ntp commit

To commit the Network Time Protocol (NTP) configuration, use the **ntp commit** command.

## **ntp commit**

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

**Defaults** None

**Command Modes** Global configuration mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to commit the NTP configuration:

```
switch# ntp commit
switch#
```

Related Commands	Command	Description
	<b>ntp abort</b>	Aborts the NTP configuration.
	<b>ntp distribute</b>	Enables Cisco Fabric Services (CFS) distribution for NTP.

# 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

<b>ip</b>	Disables IPv4 on the interface.
<b>ipv6</b>	Disables IPv6 on the interface.

## Defaults

Enabled

## Command Modes

Interface configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
6.2(2)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to disable NTP:

```
switch# ntp disable
```

## Related Commands

Command	Description
<b>ntp enable</b>	Enables NTP.



# ntp distribute

To enable Cisco Fabric Services (CFS) distribution for the 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.

**Defaults** None

**Command Modes** Global configuration mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

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

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

This example shows how to stop distribution of the active NTP configuration to the fabric:

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

Related Commands	Command	Description
	<b>ntp abort</b>	Aborts the NTP configuration.
	<b>ntp commit</b>	Commits the NTP configuration.

# ntp distribute

To enable a device to send or receive Network Time Protocol (NTP) configuration updates distributed through Cisco Fabric Services (CFS), use the **ntp distribute** command. To disable NTP distribution through CFS, use the **no** form of this command.

**ntp distribute**

**no ntp distribute**

---

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

---

**Defaults** Disabled

---

**Command Modes** Global Configuration mode

---

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

---

Command History	Release	Modification
	4.1(2)	This command was introduced.

---



---

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

In order to enable NTP distribution with CFS, you must have already enabled CFS distribution for the device using the **cfs distribute** command.

The **ntp distribute** command enables NTP to distribute its configurations through CFS. To distribute an NTP configuration change, enter the change and then use the **commit** command.

After CFS distribution is enabled for NTP, then the entry of an NTP configuration command locks the fabric for NTP until a **commit** command is entered. During the lock, no changes can be made to the NTP configuration by any other device in the fabric except the device where the lock was activated.

If CFS is disabled for NTP, then NTP does not distribute any configuration changes and does not accept a distribution from other devices in the fabric.

---

**Examples** This example shows how to enable NTP to distribute its configurations through CFS.

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ntp commit</b>	Distributes an NTP configuration change to the running configuration in all switches in the network and releases the CFS lock.
	<b>show ntp status</b>	Displays the status of NTP CFS distribution.
	<b>show cfs status</b>	Displays the global CFS distribution status (enabled/disabled) for the device.
	<b>clear ntp session</b>	Clears the application configuration session, discards pending changes, and releases the lock on the fabric.
	<b>cfs distribute</b>	Globally enables CFS distribution for all applications on the device, including CFS over IP.
	<b>ntp enable</b>	Enables the NTP protocol on a device. NTP is enabled by default.

# ntp enable

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

**ntp enable**

**no ntp enable**

---

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

---

**Defaults** Enabled

---

**Command Modes** Global configuration mode

---

**SupportedUserRoles** network-admin  
vdc-admin

---

Command History	Release	Modification
	5.2(1)	This command was deprecated.
	4.0(3)	This command was introduced.

---



---

**Usage Guidelines** NTP must be configured in the default VDC. It cannot be configured in any other VDC. This command does not require a license.

---

**Examples** This example shows how to disable NTP:

```
switch# no ntp enable
```

---

Related Commands	Command	Description
	<b>ntp server</b>	Configures a remote NTP server.

---

# 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)

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** This command does not require a license.  
Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.

**Examples** This example shows how to enable NTP logging:

```
switch# config t
switch(config)# ntp logging
switch(config)#
```

This example shows how to disable NTP logging:

```
switch# config t
switch(config)# no ntp logging
switch(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ntp logging-status</b>	Displays the NTP logging status.
<b>show ntp statistics</b>	Displays the NTP statistics.

# 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	<i>stratum</i>	(Optional) Stratum level. The range is from 1 to 15.
--------------------	----------------	--

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

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

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

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

Usage Guidelines	<p>This command enables the device to distribute time even when it is not synchronized to an existing time server.</p> <p>Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the <b>switchto vdc</b> command.</p> <p>This command does not require a license.</p>
------------------	---

Examples	<p>This example shows how to configure the device to act as an authoritative NTP server:</p>
----------	--

```
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
```

Related Commands	Command	Description
	<b>feature ntp</b>	Enables NTP on a virtual device context (VDC).
	<b>show running-config ntp</b>	Displays information about the NTP configuration that is currently running on the switch.



# 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>ipv4-address</i>	(Optional) Multicast IPv4 address.
<i>ipv6-address</i>	(Optional) Multicast IPv6 address.
<b>key</b> <i>key-id</i>	(Optional) Configures the broadcast authentication key number. The range is from 1 to 65535.
<b>ttl</b> <i>value</i>	(Optional) Configures the time-to-live (TTL) value of the multicast packets. The range is from 1 to 255
<b>version</b> <i>number</i>	(Optional) Configures the NTP version. The range is from 2 to 4.

**Defaults** None

**Command Modes** Interface configuration mode

**Supported User Roles** network-admin  
vdc-admin

Command History	Release	Modification
	6.2(2)	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
```

Related Commands	Command	Description
	<b>feature ntp</b>	Enables NTP on a virtual device context (VDC).
	<b>ntp multicast client</b>	Configures an NTP multicast client on an interface.
	<b>show running-config ntp</b>	Displays information about the NTP configuration that is currently running on the switch.

# 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

**Supported User Roles** network-admin  
vdc-admin

Command History	Release	Modification
	6.2(2)	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
```

Related Commands	Command	Description
	<b>ntp multicast</b>	Configures an NTP multicast server on an interface.
	<b>feature ntp</b>	Enables NTP on a virtual device context (VDC).
	<b>show running-config ntp</b>	Displays information about the NTP configuration that is currently running on the switch.

# ntp passive

To enable Network Time Protocol (NTP) to send synchronization responses and form associations, use the **ntp passive** command. To prevent NTP from forming associations, use the **no** form of this command.

**ntp passive**

**no ntp passive**

**Syntax Description** This command has arguments or keywords.

**Command Modes** Global configuration mode

**Supported User Roles** network-admin  
vdc-admin

Command History	Release	Modification
	6.2(2)	This command was introduced.

**Usage Guidelines** Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.

This command is available beginning with Cisco NX-OS Release 6.2(2). In previous releases, associations are enabled automatically and cannot be disabled.

This command does not require a license.

**Examples** This example shows how to enable NTP to form associations:

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

Related Commands	Command	Description
	<b>feature ntp</b>	Enables NTP on a VDC.
	<b>show running-config ntp</b>	Displays information about the NTP configuration that is currently running on the switch.

# 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*} [**key** *key-id*] [**prefer**] [**use-vrf** *vrf-name*]

**no ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**prefer**] [**use-vrf** *vrf-name*]

## Syntax Description

<i>ip-address</i>	IPv4 address.
<i>ipv6-address</i>	IPv6 address.
<i>dns-name</i>	Domain Name Server (DNS) name.
<b>key</b>	(Optional) Specifies the key to be used for associating with a server.
<i>key-id</i>	Key ID. The range is from 1 to 65535.
<b>prefer</b>	(Optional) Specifies the given NTP server as the preferred one.
<b>use-vrf</b>	(Optional) Specifies the virtual routing and forwarding (VRF) name.
<i>vrf-name</i>	VRF name. The VRF name can be <b>default</b> , <b>management</b> , or any case-sensitive, alphanumeric string up to 32 characters.

## Defaults

None

## Command Modes

Global configuration mode (config)

## Supported User Roles

network-admin  
vdc-admin  
network-operator  
vdc-operator

## Command History

Release	Modification
5.0(1)	This command was introduced.

## Usage Guidelines

Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.

You can configure multiple peer associations.

If you configure a key to be used while communicating with the NTP server, make sure that the key exists as a trusted key on the device.

This command does not require a license.

**Examples**

This example shows how to configure an NTP peer:

```
switch(config)# config t  
switch(config)# ntp peer 190.0.2.1 key 123 prefer use-vrf RED  
switch(config)#
```

This example shows how to remove an NTP peer:

```
switch# config t  
switch(config)# no ntp peer 190.0.2.1  
switch(config)#
```

**Related Commands**

Command	Description
<b>ntp server</b>	Configures an NTP server.
<b>show ntp peers</b>	Displays all the NTP peers.
<b>show ntp peer-status</b>	Displays the status for all the server/peers.

# 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} [key key-id] [prefer] [use-vrf vrf-name]
```

```
no ntp server {ip-address | ipv6-address | dns-name} [key key-id] [prefer] [use-vrf vrf-name]
```

## Syntax Description

<i>ip-address</i>	IPv4 address.
<i>ipv6-address</i>	IPv6 address.
<i>dns-name</i>	Domain Name Server (DNS) name.
<b>key</b>	(Optional) Specifies the key to be used for associating with a server.
<i>key-id</i>	Key ID. The range is from 1 to 65535.
<b>prefer</b>	(Optional) Specifies the given NTP server as the preferred one.
<b>use-vrf</b>	(Optional) Specifies the virtual routing and forwarding (VRF) name.
<i>vrf-name</i>	VRF name. The VRF name can be <b>default</b> , <b>management</b> , or any case-sensitive, alphanumeric string up to 32 characters.

## Defaults

None

## Command Modes

Global configuration mode (config)

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
5.0(1)	This command was introduced.

## Usage Guidelines

Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.

If you configure a key to be used while communicating with the NTP server, make sure that the key exists as a trusted key on the device.

This command does not require a license.



**Examples**

This example shows how to configure an NTP server:

```
switch(config) config t  
switch(config)# ntp server 190.0.2.10 key 123 prefer use-vrf RED  
switch(config)#
```

This example shows how to remove an NTP server:

```
switch# config t  
switch(config)# no ntp server 190.0.2.10 key 123 prefer use-vrf RED  
switch(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ntp peer</b>	Configures a device as an NTP peer.
<b>show ntp peer-status</b>	Displays the status of all NTP servers and peers.
<b>show ntp peers</b>	Displays all the NTP peers.

# 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*

<b>Syntax Description</b>	<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.
---------------------------	-------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Global configuration mode (config)
----------------------	------------------------------------

<b>Supported User Roles</b>	network-admin vdc-admin
-----------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to configure the NTP source:

```
switch(config)# ntp source 192.0.2.3
```

This example shows how to remove the NTP source:

```
switch(config)# no ntp source 192.0.2.3
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ntp source</b>	Displays information about the NTP source.

# 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** *if\_index*

**no ntp source-interface** *if\_index*

Syntax	Description
<i>if_index</i>	Source interface.

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

Command Modes	Global configuration mode (config)
---------------	------------------------------------

Supported User Roles	network-admin vdc-admin
----------------------	----------------------------

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

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

**Examples** This example shows how to configure an NTP source interface:

```
switch(config)# ntp source-interface loopback 1
switch(config)#
```

This example shows how to remove an NTP source configuration:

```
switch(config)# no ntp source-interface loopback 1
switch(config)#
```

Command	Description
<b>show ntp source-interface</b>	Displays information about the NTP source interface.

# ntp sync-retry

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

## ntp sync-retry

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to resynchronize NTP:

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

Related Commands	Command	Description
	ntp server	Configures a remote NTP server.

# 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*

<b>Syntax Description</b>	<i>number</i>	Trusted key number. The range is from 1 to 65535.
---------------------------	---------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Global configuration mode (config)
----------------------	------------------------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(1)	This command was introduced.

<b>Usage Guidelines</b>	Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the <b>switchto vdc</b> command.
-------------------------	---

This command provides protection against accidentally synchronizing the device to a time source that is not trusted.

This command does not require a license.

<b>Examples</b>	This example shows how to configure an NTP trusted key:
-----------------	---

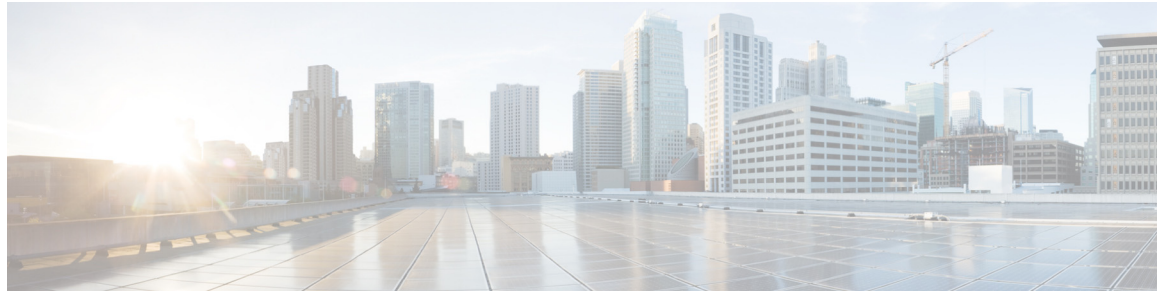
```
switch# config t
switch(config)# ntp trusted-key 42
switch(config)#
```

This example shows how to remove the NTP trusted key:

```
switch# config t
switch(config)# no ntp trusted-key 42
switch(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ntp trusted-keys</b>	Displays the status of NTP authentication.



# O Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter O.

# option exporter-stats timeout

To configure the NetFlow exporter resend timer, use the **option exporter-stats timeout** command. To remove the NetFlow exporter resend timer, use the **no** form of this command.

**option exporter-stats timeout** *time*

**no option exporter-stats timeout**

<b>Syntax Description</b>	<i>time</i>	Time in seconds. The range is from 1 to 86400.
<b>Defaults</b>	None	
<b>Command Modes</b>	NetFlow exporter version 9 configuration (config-flow-exporter-version-9)	
<b>Supported User Roles</b>	network-admin vdc-admin	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.
<b>Usage Guidelines</b>	This command does not require a license.	
<b>Examples</b>	<p>This example shows how to configure the NetFlow exporter resend timer:</p> <pre>switch(config)# flow exporter Custom-Flow-Exporter-1 switch(config-flow-exporter)# version 9 switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200 switch(config-flow-exporter-version-9)#</pre> <p>This example shows how to remove the NetFlow exporter resend timer configuration:</p> <pre>switch(config-flow-exporter-version-9)# no option exporter-stats timeout switch(config-flow-exporter-version-9)#</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show flow exporter</b>	Displays information about NetFlow exporters.



# option interface-table timeout

To configure the NetFlow exporter interface-table timer, use the **option interface-table timeout** command. To remove the interface-table timer, use the **no** form of this command.

**option interface-table timeout** *time*

**no option interface-table timeout** [*time*]

<b>Syntax Description</b>	<i>time</i>	Time in seconds. The range is from 1 to 86400.
<b>Defaults</b>	None	
<b>Command Modes</b>	NetFlow exporter version 9 configuration (config-flow-exporter-version-9)	
<b>SupportedUserRoles</b>	network-admin vdc-admin	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.
<b>Usage Guidelines</b>	This command does not require a license.	
<b>Examples</b>	<p>This example shows how to configure the NetFlow exporter interface-table timer:</p> <pre>switch(config)# flow exporter Custom-Flow-Exporter-1 switch(config-flow-exporter)# version 9 switch(config-flow-exporter-version-9)# option interface-table timeout 1200 switch(config-flow-exporter-version-9)#</pre> <p>This example shows how to remove the NetFlow exporter interface-table timer configuration:</p> <pre>switch(config-flow-exporter-version-9)# no option interface-table timeout</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show flow exporter</b>	Displays information about the NetFlow exporters.

# option sampler-table timeout

To configure the NetFlow exporter sampler-table timer, use the **option sampler-table timeout** command. To remove the sampler-table timer, use the **no** form of this command.

**option sampler-table timeout** *time*

**no option sampler-table timeout** [*time*]

<b>Syntax Description</b>	<i>time</i>	Time in seconds. The range is from 1 to 86400.
---------------------------	-------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	NetFlow exporter version 9 configuration (config-flow-exporter-version-9)
----------------------	---

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to configure the NetFlow exporter sampler-table timer:
-----------------	---

```
switch(config)# flow exporter Custom-Flow-Exporter-1
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# option sampler-table timeout 1200
switch(config-flow-exporter-version-9)#
```

This example shows how to remove the sampler-table timer configuration:

```
switch(config)# no option sampler-table timeout
switch(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show flow exporter</b>	Displays information about NetFlow exporters.



# P Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter P.

# port-monitor activate

To activate a Simple Network Management Protocol (SNMP) port-monitor policy, use the **port-monitor activate** command. To deactivate a port-monitor policy, use the **no** form of this command.

```
port-monitor activate [policy-name]
```

```
no port-monitor activate [policy-name]
```

<b>Syntax Description</b>	<i>policy-name</i> (Optional) Port-monitor policy. The maximum number of alphanumeric characters is 32.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Global configuration mode (config)
----------------------	------------------------------------

<b>Supported User Roles</b>	network-admin vdc-admin
-----------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.1(2)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to activate an SNMP port-monitor policy:

```
switch(config)# port-monitor name policy_1  
switch(config-port-monitor)# port-monitor activate policy_1  
switch(config)#
```

This example shows how to deactivate a port-monitor policy:

```
switch(config-port-monitor)# no port-monitor activate policy_1  
switch(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>counter</b>	Configures an individual counter.

# port-monitor enable

To enable the Simple Network Management Protocol (SNMP) port-monitor feature, use the **port-monitor enable** command. To disable the port-monitor feature, use the **no** form of this command.

**port-monitor enable**

**no port-monitor enable**

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

**Defaults** None

**Command Modes** Global configuration mode (config)

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to enable the SNMP port-monitor feature:

```
switch(config)# port-monitor enable
switch(config)#
```

This example shows how to disable the SNMP port-monitor feature:

```
switch(config)# no port-monitor enable
switch(config)#
```

Related Commands	Command	Description
	<b>port-monitor activate</b>	Activates the specified port-monitor policy.

## port-monitor name

To create a Simple Network Management Protocol (SNMP) port-monitor policy, use the **port-monitor name** command. To delete a port-monitor policy, use the **no** form of this command.

**port-monitor name** *policy-name*

**no port-monitor name** *policy-name*

Syntax Description	
	<i>policy-name</i> Policy name. The maximum number of alphanumeric characters is 32.

Defaults	
	None

Command Modes	
	Global configuration mode (config)

Supported User Roles	
	network-admin vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines	
	This command does not require a license.

Examples	
	This example shows how to create an SNMP port-monitor policy:

```
switch(config)# port-monitor name PM1
switch(config-port-monitor)#
```

This example shows how to remove an SNMP port-monitor policy:

```
switch(config)# no port-monitor name PM1
switch(config)
```

Related Commands	Command	Description
	<b>port-monitor activate</b>	Activates the specified port-monitor policy.

# port-type

To configure a port type for the Simple Network Management Protocol (SNMP) port monitoring, use the **port-type** command. To delete the port-type configuration for port monitoring, use the **no** form of this command.

```
port-type { access-port | all | trunks }
```

```
no port-type { access-port | all | trunks }
```

## Syntax Description

<b>access-port</b>	Configures port monitoring for access ports.
<b>all</b>	Configures port monitoring for all ports.
<b>trunks</b>	Configures port monitoring for trunk ports.

## Defaults

None

## Command Modes

Port-monitor configuration (config-port-monitor)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.1(2)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure a port type for the SNMP port-monitor configuration:

```
switch(config)# port-monitor name PM1
switch(config-port-monitor)# port-type all
switch(config-port-monitor)#
```

This example shows how to remove a port-type configuration:

```
switch(config-port-monitor)# no port-type all
switch(config-port-monitor)#
```

## Related Commands

Command	Description
<b>port-monitor activate</b>	Activates the specified port-monitor policy.

# power efficient-ethernet

To enable Energy Efficient Ethernet (EEE) for the port or port range, use the **power efficient-ethernet** command. To disable this feature, use the **no** form of this command.

**power efficient-ethernet auto | sleep threshold aggressive**

**no power efficient-ethernet auto | sleep threshold aggressive**

## Syntax Description

<b>auto</b>	Specifies auto negotiation for EEE.
<b>sleep</b>	Specifies the EEE low power idle sleep configuration.
<b>threshold</b>	Specifies the EEE low power idle sleep threshold.
<b>aggressive</b>	Specifies the EEE low power idle aggressive sleep mode.

## Defaults

no power efficient-ethernet (that is EEE is off).

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
6.1(2)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to enable auto negotiation for EEE for the port or port range:

```
switch(config-if)# power efficient-ethernet auto
ERROR: Ethernet2/1: Port is not capable of Energy Efficient Ethernet
```

This example shows how to enable EEE LPI threshold aggressive sleep mode:

```
switch(config-if)# power efficient-ethernet sleep threshold aggressive
ERROR: Ethernet2/1: Port is not capable of Energy Efficient Ethernet
```

## Related Commands

Command	Description
<b>show module</b>	Displays information about a module.



# poweroff module

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

**poweroff module** *module*

**no poweroff module** *module*

Syntax Description	<i>module</i>	Module number. The range is from 1 to 18.
--------------------	---------------	---

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

Command Modes	Global configuration mode (config)
---------------	------------------------------------

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

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

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

Examples	This example shows how to power off module 2: switch# <b>poweroff module 2</b>
----------	---

Related Commands	Command	Description
	<b>show module</b>	Displays information about a module.

# power redundancy-mode

To configure the power supply redundancy mode, use the **power redundancy-mode** command. To disable this mode, use the **no** form of this command.

```
power redundancy-mode { combined [force] | insrc-redundant | ps-redundant [single-input] |
redundant }
```

```
no power redundancy-mode { combined [force] | insrc-redundant | ps-redundant [single-input]
| redundant }
```

## Syntax Description

<b>combined</b>	Specifies the combined power supply mode.
<b>force</b>	(Optional) Forces the device to choose the combined mode without prompting the user.
<b>insrc-redundant</b>	Specifies the input source redundancy mode.
<b>ps-redundant</b>	Specifies the power supply redundancy mode.
<b>single-input</b>	(Optional) Specifies a single power input.
<b>redundant</b>	Specifies the full redundancy mode.

## Defaults

ps-redundant

## Command Modes

Global configuration mode (config)

## Supported User Roles

network-admin

Release	Modification
4.2(1)	This command was introduced.

## Usage Guidelines

You can use the **power redundancy-mode** command only in the default virtual device context (VDC).

You can configure the power supplies with the following modes:

- Combined mode—This mode does not provide power redundancy. The available power for this mode is the total power capacity of all power supplies.
- Input source redundancy mode—This mode utilizes two electrical grids, each one powering a half module within each power supply. If one power grid goes down, each power supply continues to draw power through its other half module. The available power is the amount of power by the lesser of the two grids through the power supplies.
- Power supply redundancy mode—This mode provides an extra power supply in case an active power supply goes down. The power supply that can supply the most power operates in standby mode. The other one or two power supplies are active. The available power is the amount of power provided by the active power supply units.

- Full redundancy mode—This mode combines power supply redundancy and input source redundancy, which means that the chassis has an extra power supply and one half of each power supply is connected to one electrical grid while the other half of each power supply is connected to the other electrical grid. The available power is the lesser of the available power for power supply redundancy mode and input source redundancy mode.

This command does not require a license.

---

**Examples**

This example shows how to configure the power supply redundancy mode:

```
switch# config t  
switch(config)# power redundancy-mode ps-redundant
```

This example shows how to disable the power supply redundancy mode:

```
switch# config t  
switch(config)# no power redundancy-mode ps-redundant
```

---

**Related Commands**

Command	Description
<b>show environment power</b>	Displays information about the power capacity and power distribution of the system.

# 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

<b>interval</b>	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.
<b>timeout</b>	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.

## Defaults

PTP announce interval: 1 (one packet every 2 seconds)

PTP announce timeout: 3

## Command Modes

Interface configuration mode (config-if)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
5.2(1)	This command was introduced.

## Usage Guidelines

Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.

Make sure that you have globally enabled PTP on the device 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 5/1
switch(config-if)# ptp announce interval 1
switch(config-if)#
```

This example shows how to remove the interval configuration for PTP messages:

```
switch(config)# interface ethernet 5/1
switch(config-if)# no ptp announce interval 1
switch(config-if)#
```

**Related Commands**

Command	Description
<b>ptp</b>	Enables or disables PTP on an interface.
<b>ptp delay-request minimum interval</b>	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.
<b>ptp sync interval</b>	Configures the interval between PTP synchronization messages on an interface.
<b>ptp vlan vlan</b>	Configures the PTP VLAN value on an interface.

## 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*

<b>Syntax Description</b>	<i>seconds</i>	Log seconds. The range is from -1 to 6.
---------------------------	----------------	---

<b>Defaults</b>	2 (one packet every 4 seconds).
-----------------	---------------------------------

<b>Command Modes</b>	Interface configuration mode (config-if)
----------------------	--

<b>Supported User Roles</b>	network-admin vdc-admin
-----------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.2(1)	This command was introduced.

<b>Usage Guidelines</b>	Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the <b>switchto vdc</b> command.
-------------------------	---

Make sure that you have globally enabled PTP on the device and configured the source IP address for PTP communication.

This command does not require a license.

<b>Examples</b>	This example shows how to configure the minimum interval allowed between PTP delay-request messages:
-----------------	--

```
switch# configure terminal
switch(config)# interface ethernet 5/1
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(config)# interface ethernet 5/1
switch(config-if)# no ptp delay-request minimum interval 3
switch(config-if)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ptp</b>	Enables or disables PTP on an interface.
<b>ptp announce</b>	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.
<b>ptp sync interval</b>	Configures the interval between PTP synchronization messages on an interface.
<b>ptp vlan vlan</b>	Configures the PTP VLAN value on an interface.

# 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*

<b>Syntax Description</b>	<i>domain_number</i>	Domain number. The range is from 0 to 28.
---------------------------	----------------------	---

<b>Defaults</b>	0
-----------------	---

<b>Command Modes</b>	Global configuration mode (config)
----------------------	------------------------------------

<b>Supported User Roles</b>	network-admin vdc-admin
-----------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.2(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	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(config)# no ptp domain 6
switch(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>feature ptp</b>	Enables or disables PTP on the device.
	<b>ptp source</b>	Configures the source IP address for all PTP packets.
	<b>ptp priority1</b>	Configures the priority1 value to use when advertising this clock.
	<b>ptp priority2</b>	Configures the priority2 value to use when advertising this clock.



<b>Command</b>	<b>Description</b>
<b>show ptp brief</b>	Displays the PTP status.
<b>show ptp clock</b>	Displays the properties of the local clock.

# ptp encapsulation

To configure an encapsulation for the Precision Time Protocol (PTP), use the **ptp encapsulation** command. To deactivate the encapsulation, use the **no** form of this command.

**ptp encapsulation {layer-2 | layer 3}**

**no ptp encapsulation {layer-2 | layer 3}**

Syntax Description	layer-2	layer-3
	Configures Layer 2 encapsulation. PTP packets are encapsulated within the Ethernet frame. Layer 2 encapsulation is supported in Audio Video Bridging feature.	Configures Layer 3 encapsulation. PTP packets are encapsulated with IP + UDP frame.

**Defaults** PTP is configured in Layer 2 encapsulation.

**Command Modes** Global configuration mode (config)

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

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

**Examples** This example shows how to configure PTP Layer 2 encapsulation:

```
switch# configure terminal
switch(config)# ptp encapsulation layer-2
switch(config)#
```

Related Commands	Command	Description
	<b>ptp mode</b>	Configures the PTP device mode.
	<b>ptp switchlatency-estimated</b>	Configures the maximum estimate switch latency value in nano-secs (ns).
	<b>show ptp corrections</b>	Displays the latest few corrections on this node.
	<b>show ptp parent</b>	Displays parent clock information.
	<b>show ptp time-property</b>	Displays local clock time property information.
	<b>show ptp clock</b>	Displays the properties of the local clock.

# ptp mode

To configure the Precision Time Protocol (PTP) device mode, use the **ptp mode** command. To deactivate the device mode, use the **no** form of this command.

**ptp mode** {**boundary-clock** | **generalized-ptp** | **transparent-clock**}

**no ptp mode** {**boundary-clock** | **generalized-ptp** | **transparent-clock**}

## Syntax Description

<b>boundary-clock</b>	Configures the boundary clock mode.
<b>generalized-ptp</b>	Configures the Generalized PTP (gPTP) mode. This mode is used for Audio Video Bridging feature.
<b>transparent-clock</b>	Configures the transparent clock mode. This peer-to-peer mode is added for experimental purpose, not supported officially.

## Defaults

PTP is configured in boundary-clock mode.

## Command Modes

Global configuration mode (config)

## Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

## Examples

This example shows how to configure PTP mode:

```
switch# configure terminal
switch(config)# ptp mode generatlized-ptp
switch(config)#
```

## Related Commands

Command	Description
<b>ptp encapsulation</b>	Configures an encapsulation.
<b>ptp switchlatency-estimated</b>	Configures the maximum estimate switch latency value in nano-secs (ns).
<b>show ptp corrections</b>	Displays the latest few corrections on this node.
<b>show ptp delay-summary</b>	Displays link delay and residency delay information for all interfaces. It is used in AVB.
<b>show ptp parent</b>	Displays parent clock information.

## ptp switchlatency-estimated

To configure the maximum estimate switch latency value for Precision Time Protocol (PTP), use the **ptp switchlatency-estimated** command. To reset the maximum estimate switch latency value, use the **no** form of this command.

**ptp switchlatency-estimated** *value*

**no ptp switchlatency-estimated** *value*

<b>Syntax Description</b>	<i>value</i>	The maximum estimate switch latency value. It is used in AVB. Range: 0 to 2147483647 ns. Default: 5000 ns.
---------------------------	--------------	--

<b>Defaults</b>	None.
-----------------	-------

<b>Command Modes</b>	Global configuration mode (config)
----------------------	------------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.3(0)D1(1)	This command was introduced.

**Examples** This example shows how to configure the estimated value for switch latency:

```
switch# configure terminal
switch(config)# ptp switchlatency-estimated 1
switch(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ptp encapsulation</b>	Configures an encapsulation.
	<b>ptp mode</b>	Configures the PTP device mode
	<b>show ptp corrections</b>	Displays the latest few corrections on this node.
	<b>show ptp parent</b>	Displays parent clock information.

# 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.

Defaults	255
----------	-----

Command Modes	Global configuration mode (config)
---------------	------------------------------------

Supported User Roles	network-admin vdc-admin
----------------------	----------------------------

Command History	Release	Modification
	5.2(1)	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
```

This example shows how to remove the priority1 value when advertising the PTP clock:

```
switch# configure terminal
switch(config)# no ptp priority1 10
```

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

# 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
```

<b>Syntax Description</b>	<i>priority-number</i> Priority number. The range is from 0 to 255.										
<b>Defaults</b>	255										
<b>Command Modes</b>	Global configuration mode (config)										
<b>Supported User Roles</b>	network-admin vdc-admin										
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>5.2(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	5.2(1)	This command was introduced.						
Release	Modification										
5.2(1)	This command was introduced.										
<b>Usage Guidelines</b>	This command does not require a license.										
<b>Examples</b>	<p>This example shows how to configure the priority2 value when advertising the PTP clock:</p> <pre>switch# <b>configure terminal</b> switch(config)# <b>ptp priority2 1</b></pre> <p>This example shows how to remove the priority2 value configuration for use when advertising the PTP clock:</p> <pre>switch# <b>configure terminal</b> switch(config)# <b>no ptp priority2 1</b></pre>										
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>feature ptp</b></td> <td>Enables or disables PTP on the device.</td> </tr> <tr> <td><b>ptp source</b></td> <td>Configures the source IP address for all PTP packets.</td> </tr> <tr> <td><b>ptp domain</b></td> <td>Configures the domain number to use for this clock.</td> </tr> <tr> <td><b>ptp priority1</b></td> <td>Configures the priority1 value to use when advertising this clock.</td> </tr> </tbody> </table>	Command	Description	<b>feature ptp</b>	Enables or disables PTP on the device.	<b>ptp source</b>	Configures the source IP address for all PTP packets.	<b>ptp domain</b>	Configures the domain number to use for this clock.	<b>ptp priority1</b>	Configures the priority1 value to use when advertising this clock.
Command	Description										
<b>feature ptp</b>	Enables or disables PTP on the device.										
<b>ptp source</b>	Configures the source IP address for all PTP packets.										
<b>ptp domain</b>	Configures the domain number to use for this clock.										
<b>ptp priority1</b>	Configures the priority1 value to use when advertising this clock.										

<b>Command</b>	<b>Description</b>
<b>show ptp brief</b>	Displays the PTP status.
<b>show ptp clock</b>	Displays the properties of the local clock.

## 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-id]
```

```
no ptp source ip_address [vrf vrf-id]
```

Syntax Description		
	<i>ip_address</i>	IPv4 address of the source.
	<b>vrf</b>	Specifies the VRF to be used for hello messages.
	<i>vrf-id</i>	Specifies the VRF ID.

**Defaults** None

**Command Modes** Global configuration mode (source)

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	6.1(1)	<b>vrf</b> option is deprecated in Cisco NX-OS 6.1(1) release.
	5.2(1)	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 PTP packets:

```
switch# configure terminal
switch(config)# ptp source 10.1.1.1
switch(config)#
```

This example shows how to remove the global source configuration for all PTP packets:

```
switch(config)# no ptp source 10.1.1.1
switch(config)#
```

Related Commands	Command	Description
	<b>feature ptp</b>	Enables or disables PTP on the device.
	<b>ptp domain</b>	Configures the domain number to use for this clock.



<b>Command</b>	<b>Description</b>
<b>ptp priority1</b>	Configures the priority1 value to use when advertising this clock.
<b>ptp priority2</b>	Configures the priority2 value to use when advertising this clock.
<b>show ptp brief</b>	Displays the PTP status.
<b>show ptp clock</b>	Displays the properties of the local clock.

# 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

*seconds* Log seconds. The range is from -1 to 2.

## Defaults

2 (one packet every 4 seconds)

## Command Modes

Interface configuration mode (config-if)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
5.2(1)	This command was introduced.

## Usage Guidelines

Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.

Make sure that you have globally enabled PTP on the device 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 synchronization messages on an interface:

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

This example shows how to remove the interval configuration for PTP messages synchronization:

```
switch(config)# interface ethernet 5/1
switch(config-if)# no ptp sync interval 1
switch(config-if)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ptp</b>	Enables or disables PTP on an interface.
	<b>ptp announce</b>	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.
	<b>ptp delay-request minimum interval</b>	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.
	<b>ptp vlan vlan</b>	Configures the PTP VLAN value on an interface.

# ptp vlan

To configure the Precision Time Protocol (PTP) VLAN value on an interface, use the **ptp vlan** command. To remove the PTP VLAN value from an interface, use the **no** form of this command.

**ptp vlan** *vlan-number*

**no ptp vlan** *vlan-number*

<b>Syntax Description</b>	<i>vlan-number</i>	VLAN number. The range is from 1 to 4094.
---------------------------	--------------------	---

<b>Defaults</b>	1
-----------------	---

<b>Command Modes</b>	Interface configuration mode (config-if)
----------------------	--

<b>Supported User Roles</b>	network-admin vdc-admin
-----------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.2(1)	This command was introduced.

<b>Usage Guidelines</b>	Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the <b>switchto vdc</b> command.
-------------------------	---

Make sure that you have globally enabled PTP on the device and configured the source IP address for PTP communication.

This command does not require a license.

<b>Examples</b>	This example shows how to configure the PTP VLAN value on an interface:
-----------------	---

```
switch# configure terminal
switch(config)# interface ethernet 5/5
switch(config-if)# ptp vlan 9
switch(config-if)#
```

This example shows how to remove the PTP VLAN value from an interface:

```
switch(config)# interface ethernet 5/5
switch(config-if)# no vlan 9
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ptp</b>	Enables or disables PTP on an interface.
	<b>ptp announce</b>	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.
	<b>ptp delay-request minimum interval</b>	Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.
	<b>ptp sync interval</b>	Configures the interval between PTP synchronization messages on an interface.





## R Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter R.

# rate-limit

To configure the source rate limit for Ethernet Switched Port Analyzer (SPAN) packets in the specified SPAN session, use the **rate-limit** command. To remove the rate limit configuration, use the **no** form of this command.

```
rate-limit { auto | 1-100 }
```

```
no rate-limit
```

## Syntax Description

<b>auto</b>	Automatically calculates the rate limit on a per gigabyte basis as follows: destination bandwidth/aggregate source bandwidth.
<b>1-100</b>	Specifies the percentage of the maximum rate of SPAN packets that can be sent out from each forwarding engine on a line card. The range is from 1 to 100.

## Defaults

Disabled

## Command Modes

Monitor configuration (config-monitor)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
5.2(1)	This command was introduced.

## Usage Guidelines

Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the **switchto vdc** command.

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



### Note

SPAN rate limit is supported only on F1 Series modules and F2 Series modules.

This command does not require a license

## Examples

This example shows how to configure the rate limit for SPAN packets in the specified SPAN session:

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# rate-limit 30
```



```
switch(config-monitor)#
```

This example shows how to remove the rate limit configuration for SPAN packets in the specified SPAN session:

```
switch# configure terminal  
switch(config)# monitor session 3  
switch(config-monitor)# no rate-limit
```

**Related Commands**

Command	Description
<b>monitor session</b>	Places you in the monitor configuration mode for configuring a SPAN session.
<b>show monitor session</b>	Displays the status of the SPAN or ERSPAN session.

# record

To specify a flow record to be used by a NetFlow monitor, use the **record** command. To remove the record, use the **no** form of this command.

**record** *name*

**no record** [*name*]

Syntax Description	<i>name</i>	Name of an existing NetFlow record.
--------------------	-------------	-------------------------------------

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

Command Modes	NetFlow monitor configuration (config-flow-record)
---------------	--

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

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

Usage Guidelines	Make sure that you are in the correct virtual device context (VDC). To change the VDC, use the <b>switchto vdc</b> command.
------------------	---

This command does not require a license.

Examples	This example shows how to specify a NetFlow record to use for a NetFlow monitor:
----------	--

```
switch(config)# switch(config)# flow monitor newflow1
switch(config-flow-monitor)# description recordflow
switch(config-flow-monitor)# record netflow ipv6 original-input
switch(config-flow-monitor)#
```

This example shows how to remove a record from a NetFlow monitor:

```
switch(config-flow-record)# no record netflow ipv4 original-input
switch(config-flow-record)#
```

Related Commands	Command	Description
	<b>show flow sw-monitor</b>	Displays information about NetFlow monitors.

# record netflow

To select a traditional Layer 2 record for the NetFlow monitor, use the **record netflow** command. To remove the record selection, use the **no** form of this command.

**record netflow layer2-switched input**

**no record netflow layer2-switched input**

Syntax Description		
	<b>layer2-switched</b>	Specifies the traditional Layer 2 NetFlow collection scheme.
	<b>input</b>	Specifies the input NetFlow.

**Defaults** None

**Command Modes** NetFlow monitor configuration

**Supported User Roles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0	This command was introduced.

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

**Examples** This example shows how to select a traditional Layer 2 record for the NetFlow monitor:

```
switch(config)# flow monitor FLOWMonitor1
switch(config-flow-monitor)# record netflow layer2-switched input
switch(config-flow-monitor)#
```

This example shows how to remove the traditional Layer 2 NetFlow record selection:

```
switch(config-flow-monitor)# no record netflow layer2-switched input
switch(config-flow-monitor)#
```

Related Commands	Command	Description
	<b>record</b>	Specifies a flow record to be used by a NetFlow monitor.
	<b>record netflow-original</b>	Selects an input IPv4 record.

# record netflow ipv4

To select an IPv4 record for the NetFlow monitor, use the **record netflow ipv4** command. To remove the record selection, use the **no** form of this command.

```
record netflow ipv4 { original-input | original-output | protocol-port }
```

```
no record netflow ipv4 { original-input | original-output | protocol-port }
```

## Syntax Description

<b>original-input</b>	Specifies the traditional IPv4 input NetFlow.
<b>original-output</b>	Specifies the traditional IPv4 output NetFlow.
<b>protocol-port</b>	Specifies the protocol and ports aggregation scheme.

## Defaults

None

## Command Modes

NetFlow monitor configuration (config-flow-monitor)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to select a NetFlow IPv4 record for the NetFlow monitor:

```
switch(config)# switch(config)# flow monitor newflow1
switch(config-flow-monitor)# description recordflow
switch(config-flow-monitor)# record netflow ipv4 original-input
switch(config-flow-monitor)#
```

This example shows how to remove the NetFlow IPv4 record selection:

```
switch(config-flow-monitor)# no record netflow ipv4 original-input
```

## Related Commands

Command	Description
<b>show flow sw-monitor</b>	Displays information about NetFlow monitors.

# record netflow ipv6

To select a NetFlow IPv6 record for the NetFlow monitor, use the **record netflow ipv6** command. To remove the record selection, use the **no** form of this command.

```
record netflow ipv6 { original-input | original-output | protocol-port }
```

```
no record netflow ipv6 { original-input | original-output | protocol-port }
```

## Syntax Description

<b>original-input</b>	Specifies the traditional IPv6 input NetFlow.
<b>original-output</b>	Specifies the traditional IPv6 output NetFlow.
<b>protocol-port</b>	Specifies the protocol and ports aggregation scheme.

## Defaults

None

## Command Modes

NetFlow monitor configuration (config-flow-monitor)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.1(3)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to select a NetFlow IPv6 record for the NetFlow monitor:

```
switch(config)# flow monitor Custom-NetFlow-Record-1  
switch(config-flow-monitor)# record netflow ipv6 original-input
```

This example shows how to remove the NetFlow IPv6 record selection:

```
switch(config-flow-monitor)# no record netflow ipv6 original-input  
switch(config-flow-monitor)#
```

## Related Commands

Command	Description
<b>show flow sw-monitor</b>	Displays information about NetFlow monitors.

# record netflow-original

To select an input IPv4 record, use the **record netflow-original** command. To remove the record selection, use the **no** form of this command.

**record netflow-original**

**no record netflow-original**

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

**Defaults** None

**Command Modes** NetFlow monitor configuration (config-flow-monitor)

**SupportedUserRoles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to select an IPv4 input record:

```
switch(config)# flow monitor Custom-NetFlow-Monitor-1
switch(config-flow-monitor)# record netflow-original
switch(config-flow-monitor)#
```

This example shows how to remove the record selection:

```
switch(config-flow-monitor)# no record netflow-original
switch(config-flow-monitor)#
```

Related Commands	Command	Description
	<b>show flow sw-monitor</b>	Displays information about NetFlow monitors.

# remote-span

To specify a remote Ethernet Switched Port Analyzer (RSPAN) VLAN as a SPAN session source, use the **remote-span** command. To remove an RSPAN VLAN as a SPAN session source, use the **no** form of this command.

**remote-span**

**no remote-span**

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

**Defaults** None

**Command Modes** Vlan configuration (config-vlan)

**SupportedUserRoles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to configure an RSPAN VLAN as a SPAN session source:

```
switch(config)# vlan 100
switch(config-vlan)# remote-span
```

This example shows how to remove an RSPAN VLAN configuration:

```
switch(config-vlan)# no remote-span
switch(config-vlan)#
```

Related Commands	Command	Description
	<b>monitor session</b>	Enters the monitor configuration mode.

# rmon alarm

To configure a 32-bit remote monitoring RMON alarm, use the **rmon alarm** command. To delete RMON alarms, use the **no** form of this command.

**rmon alarm** *alarm number mib-object sample-interval* {**absolute** | **delta**} **rising-threshold value** [*rising-event*] **falling-threshold value** [*falling-event*] [**owner alarm-owner**]

**no rmon alarm** *alarm-number*

## Syntax Description

<i>alarm number</i>	RMON alarm number. The range is from 1 to 65535.
<i>mib-object</i>	MIB object to monitor. The maximum length is 80 characters.
<i>sample-interval</i>	Sample interval in seconds. The range is from 1 to 2147483647.
<b>absolute</b>	Specifies to test each sample directly.
<b>delta</b>	Specifies to test the difference (delta) between the current and previous sample.
<b>rising-threshold value</b>	Specifies the rising threshold value. The range is from 2147483648 to 2147483647.
<i>rising-event</i>	(Optional) Event to trigger on a rising threshold crossing. The range is from 1 to 65535. If no event is specified, event 0 is used.
<b>falling-threshold value</b>	Specifies the falling threshold value. The range is from 2147483648 to 2147483647.
<i>falling-event</i>	(Optional) Event to trigger on a falling threshold crossing. The range is from 1 to 65535. If no event is specified, event 0 is used.
<b>owner alarm owner</b>	(Optional) Specifies an owner for the alarm. The maximum size is 80 characters.

## Defaults

None

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.



**Examples**

This example shows how to configure the 32-bit alarm number 20 for OID (1.3.6.1.2.1.2.2.1.14). The sample interval is 30 seconds and delta samples are tested. The rising threshold is 15 errors per sample window; reaching this level triggers event 1. The falling threshold is 0 errors in the sample window; reaching this level triggers event 0 (no action).

```
switch# config terminal  
switch(config)# rmon alarm 20 1.3.6.1.2.1.2.2.1.14.16777216 30 delta rising-threshold 15 1  
falling-threshold 0 owner cisco
```

```
switch(config)# no rmon alarm 20 1.3.6.1.2.1.2.2.1.14.16777216 30 delta rising-threshold  
15 1 falling-threshold 0 owner cisco
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>rmon event</b>	Configures an RMON event.
<b>rmon hcalarm</b>	Configures the 64-bit RMON alarm.
<b>show rmon</b>	Displays RMON configuration and logged information.

# rmon event

To configure an RMON event, use the **rmon event** command. To delete an RMON event, use the **no** form of this command.

```
rmon event event-number [description text] [log] [trap community-string] [owner owner-name]
```

```
no rmon event event-number
```

Syntax Description	
<i>event-number</i>	RMON event number. The range is from 1 to 65535.
<b>description</b> <i>text</i>	(Optional) Specifies a description of the event. The maximum length is 80 characters.
<b>log</b>	(Optional) Generates an RMON log entry in the onboard RMON log when the event is triggered by an alarm.
<b>trap</b> <i>community-string</i>	(Optional) Generates SNMP traps with the specified name when the event is triggered by an alarm. The maximum length is 32 characters.
<b>owner</b> <i>owner-name</i>	(Optional) Specifies an owner for the alarm. The maximum length is 80 characters.

**Defaults** None

**Command Modes** Global configuration mode

**Supported User Roles** network-admin  
vdc-admin

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

**Usage Guidelines** You can trigger an events created by this command with an alarm that you configured by using the **rmon alarm** or **rmon hcalarm** commands.

Events can be used by both **rmon alarm** (32-bit) and **hcalarm** (64-bit) commands.



**Note**

You may chose to load the default RMON events template configuration or you can delete these entries and create new RMON events. Until you create RMON alarm configurations, however, no alarms will be triggered by these configurations.

This command does not require a license.

**Examples**

This example shows how to configure RMON event 2 to log the onboard RMON log and send an SNMP trap to public community trap destinations:

```
switch# config terminal  
switch(config)# rmon event 2 log trap public description CriticalErrors owner cisco  
switch#
```

**Related Commands**

Command	Description
<b>rmon alarm</b>	Configures a 32-bit RMON alarm.
<b>rmon hcalarm</b>	Configures a 64-bit RMON alarm.
<b>show rmon</b>	Displays RMON configuration and logging information.

# rmon hcalarm

To configure a 64-bit RMON high-capacity alarm (hcalarm), use the **rmon hcalarm** command. To delete an rmon hcalarm, use the **no** form of this command.

```
rmon hcalarm alarm-number mib-object sample-interval {absolute | delta} {rising-threshold-high value rising-threshold-low value [rising-event] [falling-threshold-high value falling-threshold-low value [falling-event]]} [owner alarm-owner]
```

```
no rmon hcalarm alarm-number
```

Syntax Description	
<i>alarm-number</i>	RMON hcalarm number. The range is from 1 to 65535.
<i>mib-object</i>	MIB object to monitor. The maximum length is 80 alphanumeric characters.
<i>sample-interval</i>	Sample interval in seconds. The range is from 1 to 700000.
<b>absolute</b>	Specifies to test each sample directly.
<b>delta</b>	Specifies to test the difference (delta) between the current and previous sample.
<b>rising-threshold-high</b> <i>value</i>	Configures the upper 32 bits of the 64-bit rising threshold value. The range is from 0 to 4294967295.
<b>rising-threshold-low</b> <i>value</i>	Configures the lower 32 bits of the 64-bit rising threshold value. The range is from 0 to 4294967295.
<i>rising-event</i>	(Optional) Event to trigger on rising threshold crossing. The range is from 0 to 65535.
<b>falling-threshold-high</b> <i>value</i>	Configures the upper 32 bits of the 64-bit falling threshold value. The range is from 0 to 4294967295.
<b>falling-threshold-low</b> <i>value</i>	Configures the lower 32 bits of the 64-bit falling threshold value. The range is from 0 to 4294967295.
<i>falling-event</i>	(Optional) Event to trigger on a falling threshold crossing. The range is from 0 to 65535.
<b>owner</b> <i>alarm-owner</i>	(Optional) Specifies an owner for the alarm. The maximum size is 80 alphanumeric characters.

**Defaults** None

**Command Modes** Global configuration mode

**SupportedUserRoles** network-admin  
vdc-admin

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

**Usage Guidelines**

Event number 0 is a predefined null (or no operation) event. When no event is specified by the user in an alarm, this event is automatically used by the system. The event causes no action to be taken when triggered; however, the alarm is still reset. The event cannot be redefined by the user. It is a predefined event.

This command does not require a license.

**Examples**

This example shows how to configure a RMON high-capacity alarm:

```
switch# config terminal
switch(config)# rmon hcalarm 2 1.3.6.1.2.1.31.1.1.1.6.22544384 30 delta
rising-threshold-high 55 rising-threshold-low 3776798720 4 falling-threshold-high 41
falling-threshold-low 3906340864 owner cisco
```

**Related Commands**

Command	Description
<b>rmon alarm</b>	Configures a 32-bit RMON alarm.
<b>rmon hcalarm</b>	Configures a 64-bit RMON alarm.
<b>show rmon</b>	Displays RMON configuration and logging information.

# role distribute

To enable Cisco Fabric Services (CFS) to distribute role configurations, use the **role distribute** command.

## role distribute

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

**Defaults** None

**Command Modes** Global configuration mode

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to enable CFS to distribute role configurations and then display the status:

```
switch(config)# role distribute
switch(config)# show role status
Distribution: Enabled
Session State: Unlocked
```

Related Commands	Command	Description
	<b>show <i>application_name</i> status</b>	Displays the status of the specified application, including whether CFS distribution is enabled for the application.

# rollback running-config checkpoint

To implement a rollback for the configured checkpoint file, use the **rollback running-config checkpoint** command.

```
rollback running-config { checkpoint cp-name | file cp-file } [atomic | best-effort | stop-at-first-failure]
```

Syntax Description	Parameter	Description
	<b>checkpoint</b>	Rolls back the running configuration to a checkpoint.
	<i>cp-name</i>	Checkpoint name used in the checkpoint database. The name can be any alphanumeric string up to 80 characters but cannot contain spaces.
	<b>file</b>	Rolls back the running configuration to a configuration file.
	<i>cp-file</i>	Name of configuration file.
	<b>atomic</b>	(Optional) Implements a rollback only if no errors occur.
	<b>best-effort</b>	(Optional) Implements a rollback and skips any errors.
	<b>stop-at-first-failure</b>	(Optional) Implements a rollback that stops if an error occurs.

**Defaults** None

**Command Modes** Global configuration mode

**SupportedUserRoles** network-admin  
vdc-admin

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

**Usage Guidelines** The **rollback running-config checkpoint** command creates a rollback to the specified checkpoint name or file. The default rollback type is atomic.



**Note**

The running configuration may be disrupted before the rollback operation finally fails if you mistakenly roll back with the file option using a file from a different device but with the same VDC ID as the local VDC.

This command does not require a license.

**Examples** This example shows how to implement a rollback for the configured checkpoint file:

**rollback running-config checkpoint**

```
switch# rollback running-config checkpoint user-checkpoint-1 atomic  
Note: Applying config parallelly may fail Rollback verification  
Collecting Running-Config  
Generating Rollback Patch  
Executing Rollback Patch  
Generating Running-config for verification  
Generating Patch for verification  
switch(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show diff</b>	Displays the differences between the source and the destination file.
<b>rollback-patch</b>	





# S Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter S, excluding the **show** commands.

# sampler

To define a sampler and enter the sampler configuration mode, use the **sampler** command. To remove the sampler definition, use the **no** form of this command.

**sampler** *name*

**no sampler** *name*

<b>Syntax Description</b>	<i>name</i> Name of the sampler.
---------------------------	----------------------------------

<b>Defaults</b>	No samplers are defined.
-----------------	--------------------------

<b>Command Modes</b>	Global configuration mode
----------------------	---------------------------

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

**Usage Guidelines**

NetFlow sampling means that M out of N packets are sampled. When a packet is sampled and there is a NetFlow cache miss, a NetFlow cache entry is created for this flow. The first packet timestamp is updated and the statistics for the first packet are initialized (for example, the bytes are set to the number of bytes in the packet and the packet count is set to one). If there is a NetFlow cache hit when the packet is sampled, the cache for this flow is updated, which includes adding the number of bytes in the packet to the byte counter and incrementing the packet count by one.

Once you enter the **sampler** *name* command, you enter the sampler configuration mode, and the prompt changes to the following:

```
switch(config-flow-sampler)#
```

Within the sampler configuration mode, the following keywords and arguments are available to configure the flow monitor:

- **description** *description*—Provides a description for this sampler; you can add a maximum of 63 characters.
- **exit**—Exits from the current configuration mode.
- **mode** *sample-num out-of packets*—Configures the sampler mode. The valid values are as follows:
  - *sample-num*—Number of samples per sampling. The range is from 1 to 64.
  - **out-of**—Specifies the samples per packet ratio.
  - *packets*—Number of packets in each sampling. The range is from 1 to 8192.

- **no**—Negates a command or sets its defaults.

This command does not require a license.

### Examples

This example shows how to define a sampler and enter the sampler configuration mode:

```
switch(config)# sampler testsampler  
switch(config-flow-sampler)#
```

This example shows how to configure the sampler mode:

```
switch(config)# sampler testsampler  
switch(config-flow-sampler)# mode 24 out-of 1200
```

This example shows how to remove a sampler definition:

```
switch(config)# no sampler testsampler  
switch(config-flow)#
```

### Related Commands

Command	Description
<b>flow exporter</b>	Creates a flow exporter.
<b>flow monitor</b>	Creates a flow monitor.
<b>flow record</b>	Creates a flow record.

# sampling

To set the sampling range for Switched Port Analyzer (SPAN) packets, use the **sampling** command. To revert to the default settings, use the **no** form of this command.

**sampling** *range*

**no sampling**

<b>Syntax Description</b>	<i>range</i>	Sampling range. Every nth packet will be spanned. The range is from 2 to 1023.
---------------------------	--------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Sampling only applies to local SPAN (config-monitor) and ERSPAN source session (config-monitor-erspan-src) configuration.
----------------------	---

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	6.1(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to set the sampling range for the SPAN packets:

```
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# sampling 100
switch(config-monitor)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>monitor session</b>	Enters the monitor configuration mode.

# save

To save the current configuration session to a file, use the **save** command.

**save** *location*

<b>Syntax Description</b>	<i>location</i>	Location of the file. The location can be in bootflash:, slot0:, or volatile: The filename can be any alphanumeric string up to 63 characters.
---------------------------	-----------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>Supported User Roles</b>	network-admin network-operator vdc-admin vdc-operator
-----------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to save a configuration session to a file in bootflash:

```
switch# configure session myACLs
switch(config-s)# save bootflash:sessions/myACLs
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>delete</b>	Deletes a file from a location.

# 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}
```

```
no scheduler {aaa-authentication [username username] password [0 | 7] password |  
job name job-name | logfile size filesize | schedule name schedule-name}
```

Syntax Description		
<b>aaa-authentication</b>		Begins an AAA authentication exchange with a remote user.
<b>username</b> <i>username</i>		(Optional) Indicates the remote user is entering a username and specifies the username.
<b>password</b>		Indicates the remote user is entering a password for authentication.
<b>0</b>		Indicates the password is in clear text.
<b>7</b>		Indicates the password is encrypted.
<i>password</i>		Remote user's password.
<b>job name</b> <i>job-name</i>		Places you into job configuration mode for the specified job name. The maximum length of the name is 31 characters.
<b>logfile</b>		Specifies a logfile configuration.
<b>size</b> <i>filesize</i>		Specifies the size of the logfile. The range is from 16 to 1024 KB.
<b>schedule</b>		Defines a schedule for a job.
<b>name</b> <i>schedule-name</i>		Specifies the name of the schedule. The maximum length of the name is 31 characters.

**Defaults** None

**Command Modes** Job configuration

**SupportedUserRoles** network-admin  
vdc-admin

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

**Usage Guidelines** To use this command, the scheduler must already be enabled.  
To enable the scheduler, use the **feature scheduler** command.

Remote users must authenticate with the device using the **scheduler aaa-authentication** command before using this command to configure a maintenance job.

**Note**

The commands within a scheduler job must be entered in a single line separated by semicolon (;).

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 schedule a scheduler job to run daily at 1:00 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:

```
switch# config t
switch(config)# no scheduler job name backup-cfg
```

This example shows how to remove a scheduler job schedule:

```
switch# config t
switch(config)# no scheduler schedule name daily
```

This example shows how to specify the password for a remote user:

```
switch# config t
switch(config)# scheduler aaa-authentication password newpwd
```

This example shows how to specify a clear text password for a remote user:

```
switch# config t
switch(config)# scheduler aaa-authentication password 0 newpwd
```

This example shows how to specify an encrypted password for a remote user:

```
switch# config t
switch(config)# scheduler aaa-authentication password 7 newpwd2
```

This example shows how to specify a name and authentication password for a remote user:

```
switch# config t
switch(config)# scheduler aaa-authentication username admin1 password newpwd3
```

Related Commands	Command	Description
	<b>feature scheduler</b>	Enables the scheduler.
	<b>show scheduler</b>	Displays scheduler information.



# shut

To shut down an Ethernet Switched Port Analyzer (SPAN) session, use the **shut** command. To enable a SPAN session, use the **no** form of this command.

**shut**

**no shut**

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

**Defaults** None

**Command Modes** Monitor-common configuration (config-monitor)

**Supported User Roles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to shut down a SPAN session:

```
switch(config)# monitor session 1
switch(config-monitor)# shut
```

This example shows how to enable a SPAN session:

```
switch(config-monitor)# no shut
switch(config-monitor)#
```

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

# sleep instance

To delay the execution of a command by a specified number of seconds in the maintenance profile, use the **sleep instance** command. You can delay multiple instances of a command. To remove the delay, use the **no** form of this command.

**sleep instance** *instance-number seconds*

**no sleep instance** *instance-number seconds*

## Syntax Description

<i>instance-number</i>	Provides a label for the configuration by specifying a particular instance number. The range is from 0 to 2177483647.
<i>seconds</i>	Specifies the number of seconds by which the execution of the command has to be delayed. The range is from 0 to 2177483647.

## Defaults

None

## Command Modes

maintenance profile configuration (config-mm-profile)

## Supported User Roles

network-admin  
vdc-admin  
network-operator  
vdc-operator

## Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to delay the execution of one command by 20 seconds and another command by 10 seconds:

```
switch# configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# interface ethernet 1/1
switch(config-mm-profile-if-verify)# no shutdown
switch(config-mm-profile-if-verify)# exit
```

```
switch(config-mm-profile)# sleep instance 1 20  
switch(config-mm-profile)# router bgp 200  
switch(config-mm-profile-router)# address-family ipv4 unicast  
switch(config-mm-profile-router-af)# redistribute direct route-map my-rmap-deny  
switch(config-mm-profile-router-af)# exit  
switch(config-mm-profile-router)# exit  
switch(config-mm-profile)# sleep instance 1 10
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>configure maintenance profile</b>	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
<b>show run mmode</b>	Displays the currently running maintenance profile configuration on a switch.
<b>show system mode</b>	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.

# snapshot create

To create a snapshot, use the **snapshot create** command.

**snapshot create** *name description*

## Syntax Description

<i>name</i>	The <i>name</i> variable can be 64 characters in length.
<i>description</i>	The <i>description</i> variable can be 256 characters in length.

## Defaults

None.

## Command History

Release	Modification
7.2.0	This command was introduced.

## Examples

This example shows how to create a snapshot:

```
switch# snapshot create snap1 For documentation purposes.
Executing show interface... Done
Executing show bgp sessions vrf all... Done
Executing show ip eigrp topology summary... Done
Executing show ipv6 eigrp topology summary... Done
Executing show vpc... Done
Executing show ip ospf vrf all... Done
Feature 'ospfv3' not enabled, skipping...
Executing show isis vrf all... Done
Snapshot 'snap1' created
switch#
```

## Related Commands

Command	Description
<b>show snapshots</b> <i>before-maintenance-mode description</i>	Displays snapshots present on the switch.
<b>snapshot delete</b>	Deletes the snapshot.
<b>show snapshot compare</b>	Compares snapshots and showing the summary and details of each feature.

# snapshot delete

To delete a single snapshot or to delete all the snapshots in a system, use the **snapshot delete** command.

```
snapshot delete {all | snapshot-name}
```

Syntax Description	all	Deletes all the snapshots in the system.
	<i>snapshot-name</i>	Deletes the specified snapshot.

**Defaults** None

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

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

**Examples** This example shows how to delete all the snapshots in a system:

```
switch# snapshot delete all
```

This example shows how to delete a specific snapshot:

```
switch # snapshot delete snapshot1
```

Related Commands	Command	Description
	<b>show snapshots</b>	Displays snapshots present on the switch.
	<b>snapshot create</b>	Generates a snapshot.
	<b>snapshot section</b>	Adds or deletes a snapshot section.

## snapshot section

To add or delete a snapshot section, use the **snapshot section** command.

```
snapshot section {add section "show-command" row-id element-key1 [element-key2] | delete
section}
```

Syntax Description	Parameter	Description
	<b>add</b>	Adds the specified snapshot section to the snapshot.
	<i>section</i>	Names the snapshot section that is added to the snapshot to display the show command output.
	<i>"show command"</i>	Specifies the <b>show</b> command. The output of this <b>show</b> command is displayed in the new snapshot section created. This <b>show</b> command has to be specified within quotation marks ("show").
	<i>row-id</i>	The row-id argument specifies the tag of each row entry of the <b>show</b> command's XML output.
	<i>element-key1</i>	Specifies the tag used to distinguish among row entries in the show command snapshot section output.
	<i>element-key2</i>	(Optional) Specifies another tag used to distinguish among row entries in the show command snapshot section output.
	<b>delete</b>	Deletes the specified snapshot section from the snapshot.

**Defaults** None.

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

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

**Examples** This example shows how to add a snapshot section that displays the output of the **show ip route detail vrf all** command to the snapshot:

```
switch# snapshot section add v4route show "show ip route detail vrf all" ROW_prefix
ipprefix
```

This example shows how to delete a snapshot section from the snapshot:

```
switch# snapshot section delete v4route
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show snapshots</b>	Displays snapshots present on the switch.
<b>snapshot create</b>	Generates a snapshot.
<b>snapshot delete</b>	Deletes snapshots.

## snmp-server aaa-user cache-timeout

To configure the Simple Network Management Protocol (SNMP) time-out value for synchronized AAA users, use the **snmp-server aaa-user cache-timeout** command. To revert to the default settings, use the **no** form of this command.

**snmp-server aaa-user cache-timeout** *seconds*

**no snmp-server aaa-user cache-timeout** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Timeout value, in seconds. The range is from 1 to 86400.
<b>Defaults</b>	3600 seconds	
<b>Command Modes</b>	Global configuration mode	
<b>SupportedUserRoles</b>	network-admin vdc-admin	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(3)	This command was introduced.
<b>Usage Guidelines</b>	This command does not require a license.	
<b>Examples</b>	This example shows how to configure the AAA user synchronization timeout value:  switch# <b>configure terminal</b> switch(config)# <b>snmp-server aaa-user cache-timeout 6000</b>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show snmp</b>	Displays information about SNMP.



# snmp-server community

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

```
snmp-server community name [group name | ro | rw]
```

```
no snmp-server community name [group name | ro | rw]
```

## Syntax Description

<i>name</i>	SNMP community string. The name can be any alphanumeric string up to 32 characters.
<b>group name</b>	(Optional) Specifies the group name to which the community belongs. The name can be any alphanumeric string up to 32 characters.
<b>ro</b>	(Optional) Sets read-only access for this community.
<b>rw</b>	(Optional) Sets read-write access for this community.

## Defaults

The default community access is read-only (**ro**).

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

Use the **snmp-server community** command to configure read-only or read-write access to the SNMP agent on the device. You can optionally configure the community for an access group or user role. For more information on user roles, see the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*.

This command does not require a license.

## Examples

This example shows how to configure a read-only SNMP community:

```
switch# configure terminal
switch(config)# snmp-server community test ro
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show snmp community</b>	Displays information about SNMP communities.
<b>show snmp group</b>	Displays information about configured user roles.

# snmp-server contact

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

```
snmp-server contact [contact-info]
```

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

<b>Syntax Description</b>	<i>contact-info</i> (Optional) SNMP contact information (sysContact). The name can be any alphanumeric string up to 255 characters.				
<b>Defaults</b>	A zero-length string				
<b>Command Modes</b>	Global configuration mode				
<b>SupportedUserRoles</b>	network-admin vdc-admin				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
<b>Usage Guidelines</b>	Use the <b>snmp-server contact</b> command to configure the SNMP sysContact variable. This command does not require a license.				
<b>Examples</b>	<p>This example shows how to configure the SNMP contact:</p> <pre>switch# <b>configure terminal</b> switch(config)# <b>snmp-server contact Jane Smith@anyplace.com</b></pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show snmp</b></td> <td>Displays information about SNMP.</td> </tr> </tbody> </table>	Command	Description	<b>show snmp</b>	Displays information about SNMP.
Command	Description				
<b>show snmp</b>	Displays information about SNMP.				

## 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] [topology
topology-name]
```

```
no snmp-server context context-name [instance instance-name] [vrf vrf-name] [topology
topology-name]
```

### Syntax Description

<i>context-name</i>	SNMP context. The name can be any alphanumeric string up to 32 characters.
<b>instance</b> <i>instance-name</i>	(Optional) Specifies a protocol instance. The name can be any alphanumeric string up to 32 characters.
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) instance. The name can be any alphanumeric string up to 32 characters.
<b>topology</b> <i>topology-name</i>	(Optional) Specifies the topology. The name can be any alphanumeric string up to 32 characters.

### Defaults

None

### Command Modes

Global configuration mode

### Supported User Roles

network-admin  
vdc-admin

### Command History

Release	Modification
4.0(2)	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.

Do not use the **instance**, **vrf**, or **topology** keywords to delete a context. If you use these keywords, you map the context to a zero-length string.

If you are using SNMPv2c, use the **snmp-server mib community-map** command to map an SNMPv2c community to an SNMP context and use the **snmp-server context** command to map this context to a logical network entity.

For more information on context mapping, see the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*.

This command does not require a license.

**Examples**

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

```
switch# configure terminal  
switch(config)# snmp-server context public1 vrf red
```

**Related Commands**

Command	Description
<b>show snmp context</b>	Displays information about SNMP contexts.
<b>snmp-server mib community-map</b>	Maps an SNMPv2c community to an SNMP context.

## 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] | bgp [cbgp2] | bridge [newroot]
[topologychange] | callhome [event-notify] [smtp-send-fail] | cfs [merge-failure]
[state-change-notif] | config [ccmCLIRunningConfigChanged] | eigrp | 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] | feature-control
[FeatureOpStatusChange] | hsrp [state-change] | license [notify-license-expiry]
[notify-license-expiry-warning] [notify-licensefile-missing] [notify-no-license-for-feature]
| link [IETF-extended-linkDown] [IETF-extended-linkUp] [cisco-extended-linkDown]
[cisco-extended-linkUp] [linkDown] [linkUp] | ospf instance-tag [lsa | rate-limit rate] |
port-security [access-secure-mac-violation] [trunk-secure-mac-violation] | rf
[redundancy_framework] | rmon [fallingAlarm | hcFallingAlarm | hcRisingAlarm |
risingAlarm] | snmp [authentication] | stpx [inconsistency] [loop-consistency]
[root-inconsistency] | sysmgr [cseFailSwCoreNotifyExtended] | upgrade
[UpgradeJobStatusNotify] [UpgradeOpNotifyOnCompletion] | zone
[default-zone-behavior-change] [merge-failure] [merge-success] [request-reject1]
[unSUPP-mem] | vtp [notifs | vlancreate | vlandelete]]
```

```
no snmp-server enable traps [aaa [server-state-change] | bgp [cbgp2] | bridge [newroot]
[topologychange] | callhome [event-notify] [smtp-send-fail] | cfs [merge-failure]
[state-change-notif] | config [ccmCLIRunningConfigChanged] | eigrp | 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] | feature-control
[FeatureOpStatusChange] | hsrp [state-change] | license [notify-license-expiry]
[notify-license-expiry-warning] [notify-licensefile-missing] [notify-no-license-for-feature]
| link [IETF-extended-linkDown] [IETF-extended-linkUp] [cisco-extended-linkDown]
[cisco-extended-linkUp] [linkDown] [linkUp] | ospf instance-tag [lsa | rate-limit rate] |
port-security [access-secure-mac-violation] [trunk-secure-mac-violation] | rf
[redundancy_framework] | rmon [fallingAlarm | hcFallingAlarm | hcRisingAlarm |
risingAlarm] | snmp [authentication] | stpx [inconsistency] [loop-consistency]
[root-inconsistency] | sysmgr [cseFailSwCoreNotifyExtended] | upgrade
[UpgradeJobStatusNotify] [UpgradeOpNotifyOnCompletion] | zone
[default-zone-behavior-change] [merge-failure] [merge-success] [request-reject1]
[unSUPP-mem] | vtp [notifs | vlancreate | vlandelete]]
```

### Syntax Description

<b>aaa</b>	(Optional) Enables AAA notifications.
<b>server-state-change</b>	(Optional) Enables the server-state-change AAA notification.
<b>bgp</b>	(Optional) Enables CISCO-BGP4-MIB notifications.
<b>cbgp2</b>	(Optional) Enables CISCO-BGP-MIBv2 notifications.
<b>bridge</b>	(Optional) Enables STP bridge MIB notifications.
<b>newroot</b>	(Optional) Enables STP new root bridge notifications.
<b>topologychange</b>	(Optional) Enables STP topology change notifications.

<b>callhome</b>	(Optional) Enables Call Home notifications.
<b>event-notify</b>	(Optional) Enables Call Home external event notifications.
<b>smtp-send-fail</b>	(Optional) Enables the smtp-send-fail Simple Mail Transfer Protocol (SMTP) message send fail notifications.
<b>cfs</b>	(Optional) Enables Cisco Fabric Services (CFS) notifications.
<b>merge-failure</b>	(Optional) Enables merge failure notifications.
<b>state-change-notif</b>	(Optional) Enables state change notifications.
<b>config</b>	(Optional) Enables configuration change notifications.
<b>ccmCLIRunningConfigChanged</b>	(Optional) Enables CLI running/startup config change notifications.
<b>eigrp</b>	(Optional) Enables EIGRP4-MIB notifications.
<b>entity</b>	(Optional) Enables ENTITY-MIB notifications.
<b>entity_mib_change</b>	(Optional) Enables entity MIB change notifications.
<b>entity_module_inserted</b>	(Optional) Enables entity module inserted notifications.
<b>entity_module_removed</b>	(Optional) Enables entity module removed notifications.
<b>entity_module_status_change</b>	(Optional) Enables entity module status change notifications.
<b>entity_power_out_change</b>	(Optional) Enables entity power out change notifications.
<b>entity_power_status_change</b>	(Optional) Enables entity power status change notifications.
<b>entity_unrecognised_module</b>	(Optional) Enables entity unrecognized module notifications.
<b>feature-control</b>	(Optional) Enables feature change notifications.
<b>FeatureOpStatusChange</b>	(Optional) Enables feature operation status change notifications.
<b>hsrp</b>	(Optional) Enables CISCO-HSRP-MIB notifications.
<b>state-change</b>	(Optional) Enables the state-change HSRP notifications.
<b>license</b>	(Optional) Enables license notifications.
<b>notify-license-expiry</b>	(Optional) Enables license expiry notifications.
<b>notify-license-expiry-warning</b>	(Optional) Enables license expiry warning notifications.
<b>notify-licensefile-missing</b>	(Optional) Enables license file missing notifications.
<b>notify-no-license-for-feature</b>	(Optional) Enables no license installed for feature notifications.
<b>link</b>	(Optional) Enables IF-MIB link notifications.
<b>IETF-extended-linkDown</b>	(Optional) Enables Internet engineering task force (IETF) extended link state down notifications.
<b>IETF-extended-linkUp</b>	(Optional) Enables IETF extended link state up notifications.

<b>cisco-extended-linkDown</b>	(Optional) Enables Cisco extended link state down notifications.
<b>cisco-extended-linkUp</b>	(Optional) Enables Cisco extended link state up notifications.
<b>linkDown</b>	(Optional) Enables IETF Link state down notifications.
<b>linkUp</b>	(Optional) Enables IETF Link state up notifications.
<b>ospf <i>instance-tag</i></b>	(Optional) Enables Open Shortest Path First (OSPF) notifications.
<b>lsa</b>	(Optional) Enables OSPF LSA notifications.
<b>rate-limit <i>rate</i></b>	(Optional) Enables rate limits on OSPF notifications. The range is from 2 to 60 seconds. The default is 10 seconds.
<b>port-security</b>	(Optional) Enables port security notifications.
<b>access-secure-mac-violation</b>	(Optional) Enables secure MAC violation notifications.
<b>trunk-secure-mac-violation</b>	(Optional) Enables VLAN secure MAC violation notifications.
<b>rf</b>	(Optional) Enables redundancy framework (RF) SNMP notifications.
<b>redundancy_ framework</b>	(Optional) Enables redundancy_ framework (RF) Supervisor switchover MIB notifications.
<b>rmon</b>	(Optional) Enables remote monitoring (RMON) notifications.
<b>fallingAlarm</b>	(Optional) Enables RMON falling alarm notifications.
<b>hcFallingAlarm</b>	(Optional) Enables RMON high capacity falling alarm notifications.
<b>hcRisingAlarm</b>	(Optional) Enables RMON high capacity rising alarm notifications.
<b>risingAlarm</b>	(Optional) Enables RMON rising alarm notifications.
<b>snmp</b>	(Optional) Enables general SNMP notifications.
<b>authentication</b>	(Optional) Enables SNMP authentication notifications.
<b>stp</b>	(Optional) Enables STP MIB notifications.
<b>inconsistency</b>	(Optional) Enables SNMP STP MIB InconsistencyUpdate notifications.
<b>loop-inconsistency</b>	(Optional) Enables SNMP STP MIB Loop InconsistencyUpdate notifications.
<b>root-inconsistency</b>	(Optional) Enables SNMP STP MIB RootInconsistencyUpdate notifications.
<b>sysmgr</b>	(Optional) Enables software change notifications.
<b>cseFailSwCoreNotify Extended</b>	(Optional) Enables software core notifications.
<b>upgrade</b>	(Optional) Enables upgrade notifications.
<b>UpgradeJobStatusNotify</b>	(Optional) Enables upgrade job status notifications.
<b>UpgradeOpNotifyOn Completion</b>	(Optional) Enables upgrade global status notifications.
<b>zone</b>	(Optional) Enables default zone change notifications.
<b>default-zone-behavior-change</b>	(Optional) Enables default zone behavior change notifications.
<b>merge-failure</b>	(Optional) Enables merge failure notifications.
<b>merge-success</b>	(Optional) Enables merge success notifications.
<b>request-reject1</b>	(Optional) Enables request reject notifications.



<b>unsupp-mem</b>	(Optional) Enables unsupported member notifications.
<b>vtp</b>	(Optional) Enables VLAN Trunking Protocol (VTP) trap notifications.
<b>notifs</b>	(Optional) Enables the following notifications: vtpConfigRevNumberError, vtpConfigDigestError, vtpServerDisabled, vtpVersionOneDeviceDetected, vlanTrunkPortDynamicStatusChange, vtpLocalModeChanged, vtpVersionInUseChanged and vtpPruningStateOperChange.
<b>vlancreate</b>	(Optional) Enables vtpVlanCreated notifications.
<b>vlandelete</b>	(Optional) Enables vtpVlanDeleted notifications.

**Defaults**

License and SNMP authentication notifications are enabled.

**Command Modes**

Global configuration mode

**Supported User Roles**

network-admin  
vdc-admin

**Command History**

Release	Modification
6.2(8)	Added the <b>cbgp2</b> keyword.
5.0(2)	Added the <b>cfs</b> , <b>config</b> , <b>feature-control</b> , <b>rmon</b> , and <b>zone</b> keywords.
4.0(3)	Added the <b>eigrp</b> keyword.
4.0(2)	Added the OSPF <b>rate-limit</b> keyword.
4.0(1)	This command was introduced.

**Usage Guidelines**

This command does not require a license.

**Examples**

This example shows how to enable BGP notifications:

```
switch# configure terminal
switch(config) snmp-server enable traps bgp
```

This example shows how to enable VTP notifications:

```
switch# configure terminal
switch(config) snmp-server enable traps vtp
```

**Related Commands**

Command	Description
<b>show snmp trap</b>	Displays the enable or disable state of all SNMP notifications.

# snmp-server globalEnforcePriv

To globally enforce privacy for all Simple Network Management Protocol (SNMP) users, use the **snmp-server globalEnforcePriv** command. To disable global privacy, use the **no** form of this command.

**snmp-server globalEnforcePriv**

**no snmp-server globalEnforcePriv**

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

**Defaults** Disabled

**Command Modes** Global configuration mode

**SupportedUserRoles** network-admin  
vdc-admin

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

**Usage Guidelines** Use the **snmp-server globalEnforcePriv** command to enforce privacy on all SNMP users. This command does not require a license.

**Examples** This example shows how to globally enforce privacy for all SNMP contacts:

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

Related Commands	Command	Description
	<b>show snmp</b>	Displays information about SNMP.

# snmp-server host

To specify the server host to receive Simple Network Management Protocol (SNMP) notifications, use the **snmp-server host** command. To remove the SNMP server configuration, use the **no** form of this command.

```
snmp-server host host-name {snmp-name | filter-vrf {vrf-name | default | management}} |
informs {snmp-name | version {1 snmp-name | 2c snmp-name | 3 {auth snmp-name | noauth
snmp-name | priv snmp-name}}} | source-interface {ethernet number | loopback number |
mgmt number | port-channel number | vlan number} | traps {snmp-name | version {1
snmp-name | 2c snmp-name | 3 {auth snmp-name | noauth snmp-name | priv snmp-name}}} |
use-vrf {vrf-name | default | management} | version {1 snmp-name | 2c snmp-name | 3 {auth
snmp-name | noauth snmp-name | priv snmp-name}} | udp-port port
```

```
no snmp-server host host-name {snmp-name | filter-vrf {vrf-name | default | management}} |
informs {snmp-name | version {1 snmp-name | 2c snmp-name | 3 {auth snmp-name | noauth
snmp-name | priv snmp-name}}} | source-interface {ethernet number | loopback number |
mgmt number | port-channel number | vlan number} | traps {snmp-name | version {1
snmp-name | 2c snmp-name | 3 {auth snmp-name | noauth snmp-name | priv snmp-name}}} |
use-vrf {vrf-name | default | management} | version {1 snmp-name | 2c snmp-name | 3 {auth
snmp-name | noauth snmp-name | priv snmp-name}} | udp-port port
```

## Syntax Description

<i>host-name</i>	IP4 or IPv6 address or name of the host.
<i>snmp-name</i>	SNMP community string or SNMPv3 username. The maximum number of alphanumeric characters is 32.
<b>filter-vrf</b>	Specifies the virtual routing and forwarding (VRF) instance whose notifications are to be filtered.
<i>vrf-name</i>	Name of the VRF. The maximum number of alphanumeric characters is 32.
<b>default</b>	Specifies the default VRF.
<b>management</b>	Specifies the management VRF.
<b>informs</b>	Sends SNMP information to this host.
<b>version</b>	Specifies the SNMP version used to send notifications.
<b>1</b>	Specifies SNMPv1.
<b>2c</b>	Specifies SNMPv2c.
<b>3</b>	Specifies SNMPv3.
<b>auth</b>	Specifies the SNMPv3 authNoPriv security level.
<b>noauth</b>	Specifies the SNMPv3 noAuthNoPriv security level.
<b>priv</b>	Specifies the SNMPv3 authPriv security level.
<b>source-interface</b>	Specifies the source interface used to send SNMP notifications to this host.
<b>ethernet</b> <i>number</i>	Specifies the Ethernet IEEE 802.3z slot number and port number in this format: 1/1. The range for the slot number is from 1 to 18, and the range for the port number is from 1 to 128.
<b>loopback</b> <i>number</i>	Specifies the virtual interface number. The range is from 0 to 1023.
<b>mgmt</b> <i>number</i>	Specifies the management interface number. The value is 0.

<b>port-channel</b> <i>number</i>	Specifies the port-channel number and the subinterface number in this format: 1.1. The range for the port-channel number is from 1 to 4096, and the range for the subinterface number is from 1 to 4093.
<b>vlan</b> <i>number</i>	Specifies the VLAN interface number. The range is from 1 to 4094.
<b>traps</b>	Sends SNMP traps to this host.
<b>use-vrf</b>	Specifies the name of the VRF on which notifications are to be sent.
<b>udp-port</b> <i>port</i>	Specifies the User Datagram Protocol (UDP) port number of the notification host. The range is from 0 to 65535.

**Defaults**

None

**Command Modes**

Global configuration mode

**Supported User Roles**network-admin  
vdc-admin**Command History**

Release	Modification
4.2(1)	This command was introduced.

**Usage Guidelines**

The source-interface configuration overrides the global source-interface configuration.

This command does not require a license.

**Examples**

This example shows how to configure an SNMP server host:

```
switch(config)# snmp-server host 192.0.2.1 traps snmp1 udp-port 1
```

This example shows how to remove an SNMP server host:

```
switch(config)# no snmp-server host 192.0.2.1 traps snmp1 udp-port 1
switch(config)#
```

**Related Commands**

Command	Description
<b>snmp-server</b> <b>community</b>	Configures the SNMP community string.
<b>snmp-server</b> <b>contact</b>	Configures the SNMP contact information.

# snmp-server host filter-vrf

To configure a Simple Network Management Protocol (SNMP) host receiver to gather notifications that occur on a specific virtual routing and forwarding (VRF) instance, use the **snmp-server host filter-vrf** command. To remove the VRF filter, use the **no** form of this command.

```
snmp-server host host-address filter-vrf vrf-name [udp-port port]
```

```
no snmp-server host host-address filter-vrf vrf-name [udp-port port]
```

Syntax Description		
	<i>host-address</i>	Name or IP address of the host (the targeted recipient).
	<i>vrf-name</i>	Name of the VRF. The name can be any alphanumeric string up to 63 characters.
	<b>udp-port</b> <i>port</i>	(Optional) Specifies the port UDP port of the host to use. The range is from 0 to 65535. The default is 162.

**Defaults** None

**Command Modes** Global configuration mode

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

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

**Examples** This example shows how to configure the host receiver to receive notifications from the red VRF.

```
switch# config terminal
switch(config)# snmp-server host 10.1.1.1 filter-vrf red
```

Related Commands	Command	Description
	<b>show snmp</b>	Displays SNMP information.
	<b>snmp-server host</b>	Configures an SNMP host receiver.
	<b>snmp-server host use-vrf</b>	Configures Cisco NX-OS to send notifications on the specified VRF to communicate with an SNMP host receiver.

## snmp-server host use-vrf

To configure the device to communicate with a Simple Network Management Protocol (SNMP) host receiver on a specific virtual routing and forwarding (VRF) instance, use the **snmp-server host use-vrf** command. To return to the default, use the **no** form of this command.

**snmp-server host** *host-address* **use-vrf** *vrf-name* [**udp-port** *port*]

**no snmp-server host** *host-address* **use-vrf** *vrf-name* [**udp-port** *port*]

Syntax Description	Parameter	Description
	<i>host-address</i>	Name or IP address of the host (the targeted recipient).
	<i>vrf-name</i>	Name of the VRF. The name can be any alphanumeric string up to 63 characters.
	<b>udp-port</b> <i>port</i>	(Optional) Specifies the port UDP port of the host to use. The range is from 0 to 65535. The default is 162.

**Defaults** None

**Command Modes** Global configuration mode

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

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

**Examples** This example shows how to configure Cisco NX-OS to communicate with the host receiver on the blue VRF.

```
switch# config terminal
switch(config)# snmp-server host 10.1.1.1 use-vrf blue
```

Related Commands	Command	Description
	<b>show snmp</b>	Displays SNMP information.
	<b>snmp-server host</b>	Configures an SNMP host receiver.
	<b>snmp-server host filter-vrf</b>	Sends only notifications on the specified VRF to the host receiver.

# snmp-server location

To configure the device location used by the Simple Network Management Protocol (SNMP), use the **snmp-server location** command. To remove the location, use the **no** form of this command.

**snmp-server location** *[location]*

**no snmp-server location** *[location]*

<b>Syntax Description</b>	<i>location</i>	(Optional) System location. The location can be any alphanumeric string up to 255 characters.
<b>Defaults</b>	None	
<b>Command Modes</b>	Global configuration mode	
<b>SupportedUserRoles</b>	network-admin vdc-admin	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.
<b>Usage Guidelines</b>	This command does not require a license.	
<b>Examples</b>	This example shows how to set the SNMP location: switch# <b>config terminal</b> switch(config)# <b>snmp-server location SanJose</b>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show snmp</b>	Displays information about SNMP.

# snmp-server mib community-map

To configure the Simple Network Management Protocol (SNMP) version 2c community to context mapping, use the **snmp-server mib community-map** command. To remove the community to context 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>	SNMP community string. The string can be any alphanumeric string up to 32 characters.
<b>context</b> <i>context-name</i>	Specifies the SNMP context. The name can be any alphanumeric string up to 32 characters.

## Defaults

None

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(2)	This command was introduced.

## Usage Guidelines

Use the **snmp-server mib community-map** command to map between SNMPv2c communities and SNMP contexts. Use the **snmp-server context** command to map this context to a logical network entity.

For more information on context mapping, see the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*.

This command does not require a license.

## Examples

This example shows how to map the public community to the public1 context:

```
switch# configure terminal
switch(config)# snmp-server mib community-map public context public1
```



Related Commands	Command	Description
	<b>show snmp community</b>	Displays information about SNMP communities.
	<b>show snmp context</b>	Displays information about SNMP contexts.
	<b>snmp-server context</b>	Maps an SNMP context to a logical network entity.

## snmp-server packetsize

To establish control over the largest Simple Network Management Protocol (SNMP) packet size permitted when the SNMP server is receiving a request or generating a reply, use the **snmp-server packetsize** command. To restore the default, use the **no** form of this command.

**snmp-server packetsize** *byte-count*

**no snmp-server packetsize** *byte-count*

<b>Syntax Description</b>	<i>byte-count</i>	Range is 484 to 17382.
<b>Command Default</b>	Packet size is not configured.	
<b>Command Modes</b>	Global configuration mode	
<b>SupportedUserRoles</b>	network-admin vdc-admin	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	6.2(10)	This command was introduced.
<b>Usage Guidelines</b>	This command does not require a license.	
<b>Examples</b>	The following example establishes a packet filtering of a maximum size of 1024 bytes:  switch(config)# <b>snmp-server packetsize 1024</b>	

# snmp-server protocol enable

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

**snmp-server protocol enable**

**no snmp-server protocol enable**

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

**Defaults** Enabled

**Command Modes** Global configuration mode

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(3)	This command was introduced.

**Usage Guidelines** Use the **no snmp protocol enable** command to disable SNMP and close any TCP or UDP ports associated with the protocol.

This command does not require a license.

**Examples** This example shows how to disable SNMP:

```
switch# configure terminal
switch(config)# no snmp-server protocol enable
```

## snmp-server source-interface

To configure a Simple Network Management Protocol (SNMP) source interface through which notifications are sent, use the **snmp-server source-interface** command. To remove the SNMP source interface configuration, use the **no** form of this command.

**snmp-server source-interface** {traps | informs} {ethernet *number* | loopback *number* | mgmt *number* | port-channel *number* | vlan *number*}

**no snmp-server source-interface** {traps | informs} {ethernet *number* | loopback *number* | mgmt *number* | port-channel *number* | vlan *number*}

### Syntax Description

<b>traps</b>	Sends SNMP traps through the source interface.
<b>informs</b>	Sends SNMP information through the source interface.
<b>ethernet</b> <i>number</i>	Specifies the Ethernet IEEE 802.3z slot number and port number in this format: 1/1. The range for the slot number is from 1 to 18, and the range for the port number is from 1 to 128.
<b>loopback</b> <i>number</i>	Specifies the virtual interface number. The range is from 0 to 1023.
<b>mgmt</b> <i>number</i>	Specifies the management interface number.
<b>port-channel</b> <i>number</i>	Specifies the port-channel number and the subinterface number in this format: 1.1. The range for the port-channel number is from 1 to 4096, and the range for the subinterface number is from 1 to 4093.
<b>vlan</b> <i>number</i>	Specifies the VLAN interface number. The range is from 1 to 4094.

### Defaults

None

### Command Modes

Global configuration mode

### Supported User Roles

network-admin  
vdc-admin

### Command History

Release	Modification
4.2(1)	This command was introduced.

### Usage Guidelines

This command does not require a license.

### Examples

This example shows how to configure an SNMP source interface:

```
switch(config)# snmp-server source-interface traps ethernet 1/1
```

This example shows how to remove the SNMP source interface:

```
switch(config)# no snmp-server source-interface traps ethernet 1/1
switch(config)#
```

**Related Commands**

Command	Description
<b>snmp-server community</b>	Configures the SNMP community string.
<b>snmp-server host</b>	Configures a host receiver for SNMP notifications.

## snmp-server tcp-session

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

**snmp-server tcp-session [auth]**

**no snmp-server tcp-session [auth]**

<b>Syntax Description</b>	<b>auth</b> (Optional) Enables one-time authentication for SNMP over a TCP session.
---------------------------	---

<b>Defaults</b>	One-time authentication for SNMP over a TCP session is enabled.
-----------------	---

<b>Command Modes</b>	Global configuration mode
----------------------	---------------------------

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to enable one-time authentication for SNMP over a TCP session.
-----------------	---

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show snmp</b>	Displays information about SNMP.

# snmp-server user

To configure the Simple Network Management Protocol (SNMP) user information, use the **snmp-server user** command. To disable the configuration or to revert to factory defaults, use the **no** form of this command.

```
snmp-server user username [group-name] [auth {md5 | sha} password [priv [aes-128] password] [localizedkey] [engineID id]
```

```
no snmp-server user username [group-name] [auth {md5 | sha} password [priv [aes-128] password] [localizedkey] [engineID id]
```

## Syntax Description

<i>username</i>	Name of the user. The name can be any case-sensitive, alphanumeric string up to 32 characters.
<i>group-name</i>	(Optional) Name of the group. The name can be any case-sensitive, alphanumeric string up to 32 characters.
<b>auth</b>	(Optional) Sets authentication parameters for the user.
<b>md5</b>	Uses the MD5 algorithm for authentication.
<b>sha</b>	Uses the SHA algorithm for authentication.
<i>password</i>	User password. The password can be any case-sensitive, alphanumeric string up to 64 characters. If you configure the <b>localizedkey</b> keyword, the password can be any case-sensitive, alphanumeric string up to 130 characters
<b>priv</b>	(Optional) Sets encryption parameters for the user.
<b>aes-128</b>	(Optional) Sets the 128-byte AES algorithm for privacy.
<b>localizedkey</b>	(Optional) Sets passwords in the localized key format. If you configure this keyword, the password can be any case-sensitive, alphanumeric string up to 130 characters.
<b>engineID</b> <i>id</i>	(Optional) Configures the SNMP Engine ID for a notification target user. The engineID format is a 12-digit colon-separated decimal number.

## Defaults

None

## Command Modes

Global configuration mode

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

Use the **snmp-server user** command to configure user authentication and privacy settings for SNMP. If you use the **localizedkey** keyword, you cannot port the SNMP user configuration across devices because the user password contains information on the engine ID of the device. If you copy a configuration file

into the device, the passwords may not be set correctly if the configuration file was generated at a different device. We recommend that you explicitly configure passwords after copying the configuration into the device.

SNMP Version 3 is the most secure model, because it allows packet encryption with the **priv** keyword.

To assign multiple roles to a user, configure multiple **snmp-server user** *username group-name* commands. The *group-name* argument is defined by the **role name** command.

If you are configuring an SNMP notification target user, use the **engineID** keyword to configure the SNMP engine ID for this user.

To delete the user or the role associated with that user, use the **no** form of this command.

**Note**


---

You cannot delete the last role for a user.

---

This command does not require a license.

**Examples**

This example shows how to set the user authentication information for user jane:

```
switch# config terminal
switch(config)# snmp-server user jane network-admin auth sha abcd1234
```

This example shows how to multiple roles for user sam:

```
switch# config terminal
switch(config)# snmp-server user sam network-admin
switch(config)# snmp-server user sam testrole
```

This example shows how to set user authentication and privacy information for user Juan:

```
switch# config terminal
switch(config)# snmp-server user Juan network-admin auth sha abcd1234 priv abcdefgh
```

This example shows how to set user authentication and SNMP engine ID for a notification target user:

```
switch# config terminal
switch(config)# snmp-server user notifUser network-admin auth sha abcd1234 engineID
00:12:00:00:09:03:00:05:48:00:74:30
```

**Related Commands**

Command	Description
<b>role name</b>	Configures role profiles used as SNMP group names.
<b>show snmp</b>	Displays SNMP information.
<b>snmp-server host</b>	Configures SNMP server host information.



# snmp-server user enforcePriv

To enforce privacy for a Simple Network Management Protocol (SNMP) user, use the **snmp-server user enforcePriv** command. To revert to factory defaults, use the **no** form of this command.

**snmp-server user *username* enforcePriv**

**no snmp-server user *username* enforcePriv**

Syntax Description	<i>username</i>	Name of the user. The name can be any case-sensitive, alphanumeric string up to 32 characters.
--------------------	-----------------	--

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

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

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

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

**Examples** This example shows how to enforce privacy for the user joe:

```
switch# config terminal
switch(config)# snmp-server user joe enforcePriv
```

Related Commands	Command	Description
	<b>role name</b>	Configures role profiles used as SNMP group names.
	<b>show snmp</b>	Displays SNMP information.
	<b>snmp-server user</b>	Configures SNMP user information.

# snmp-trap

To generate a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered, use the **snmp-trap** command.

```
snmp-trap [intdata1 integer-data1] [intdata2 integer-data2] [strdata string-data] event-type
           ev_type policy-name name
```

Syntax Description		
<b>intdata1</b> <i>integer-data1</i>	(Optional) Specifies an integer to be sent in the SNMP trap message to the SNMP agent.	
<b>intdata2</b> <i>integer-data2</i>	(Optional) Specifies a second integer to be sent in the SNMP trap message to the SNMP agent.	
<b>strdata</b> <i>string-data</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.	
<b>event-type</b> <i>ev_type</i>	Specifies the event type. Event type.	
<b>policy-name</b> <i>name</i>	Specifies the policy name. Policy name.	

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

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

```
switch(config)# event manager applet snmp-applet
switch(config-applet)# action 1 snmp-trap strdata "EEM detected server failure"
switch(config-applet)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>syslog</b>	Configures a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered.

## source

To configure the NetFlow exporter interface to use to reach the NetFlow collector for the configured destination, use the **source** command. To remove the source, use the **no** form of this command.

**source** *if-type if-number*

**no source** [*if-type if-number*]

Syntax Description		
	<i>if-type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>if-number</i>	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Defaults	
	None

Command Modes	
	NetFlow exporter configuration (config-flow-exporter)

Supported User Roles	
	network-admin vdc-admin

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

Usage Guidelines	
	This command does not require a license.

Examples	
	This example shows how to configure the NetFlow exporter source interface:

```
switch(config)# flow exporter Netflow-Exporter-1
switch(config-flow-exporter)# source Ethernet3/11
switch(config-flow-exporter)#
```

This example shows how to remove the Netflow exporter source interface configuration:

```
switch(config-flow-exporter)# no source Ethernet3/11
switch(config-flow-exporter)#
```

Related Commands	Command	Description
	<b>show flow exporter</b>	Displays information about NetFlow exporters.

## source

To configure sources and the traffic direction in which to copy packets, use the **source** command. To remove sources, use the **no** form of this command.

```
source {exception {all | fabricpath | layer3 | other} | interface {all | ethernet {slot-number /  
port-number | range} | port-channel {port-channel-number | range} | sup-eth  
inband-interface-number} | vlan {number | range} [both | rx | tx]}
```

```
no source {exception {all | fabricpath | layer3 | other} | interface {all | ethernet {slot-number /  
port-number | range} | port-channel {port-channel-number | range} | sup-eth  
inband-interface-number} | vlan {number | range} [both | rx | tx]}
```

Syntax Description	
<b>exception</b>	Specifies exception sources. You can specify <b>all</b> , <b>fabricpath</b> , <b>layer3</b> and <b>other</b> sources as exception sources.
<b>interface</b>	Specifies interfaces. Use the <b>all</b> keyword to enable the monitor session to monitor all VLANs and ports in the VDC such as physical ports, Port Channels, FEX ports and FEX Port Channels. The <b>all</b> keyword is supported only in extended SPAN and extended ERSPAN sessions.
<b>ethernet</b>	Specifies ethernet interfaces.
<i>slot-number</i>	Specifies the slot-number. The range is from 1 to 253.
<i>port-number</i>	Specifies the port-number. The range is from 1 to 254.
<i>range</i>	Specifies the range.
<b>port-channel</b>	Specifies port-channel interfaces.
<i>port-channel-number</i>	Specifies the port-channel number. The range is from 1 to 4096.
<b>sup-eth</b>	Specifies the ethernet inband interface.
<i>inband-interface-number</i>	Specifies the ethernet inband interface number. You can only specify the value as 0.
<b>vlan</b>	Specifies a VLAN.
<i>number</i>	Specifies the VLAN number. The range is from 1 to 3967.
<b>rx</b>	Specifies traffic direction as ingress.
<b>tx</b>	Specifies traffic direction as egress.
<b>both</b>	Specifies traffic direction as both ingress and egress.

**Defaults** None

**Command Modes** Monitor configuration (config- monitor)

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator

vdc-operator

### Command History

Release	Modification
7.3(0)D1(1)	You can use the <b>all</b> keyword to enable the monitor session to monitor all VLANs and ports in the VDC such as physical ports, Port Channels, FEX ports and FEX Port Channels.
4.0(1)	This command was introduced.

### Usage Guidelines

You can configure one or more sources, as either a series of comma-separated entries, or a range of numbers. You can specify up to 128 interfaces.

This command does not require a license.

### Examples

This example shows how to configure sources and the traffic direction in which to copy packets:

```
switch(config)# monitor session 1
switch(config-monitor)# source vlan 3, 6-10 tx

switch(config)# monitor session 2
switch(config-monitor)# source interface sup-eth 0 both

switch(config)# monitor session 2
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
```

This example shows how to remove a source configuration:

```
switch(config-monitor)# no source vlan 3, 6-10 tx
```

This example shows how to enable the monitor session to monitor all VDC ports:

```
switch(config)# monitor session 2
switch(config-monitor)# source interface all rx
```

### Related Commands

Command	Description
<b>show monitor session</b>	Displays the virtual SPAN or ERSPAN configuration.
<b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

# source exception

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

```
source exception {layer3 | fabricpath | other | all}
```

```
no source exception {layer3 | fabricpath | other | all}
```

## Syntax Description

<b>layer3</b>	Specifies the Layer 3 exception type for F2 Series and M Series modules.
<b>fabricpath</b>	Specifies the FabricPath exception type for F Series modules.
<b>other</b>	Specifies exceptions for M Series modules that are dropped through redirect registers programmed with a drop destination interface.
<b>all</b>	Includes all Layer 3, FabricPath, and other exceptions.

## Defaults

None

## Command Modes

config-monitor mode (for a SPAN session)  
 config-erspan-src mode (for an ERSPAN session)

## Supported User Roles

network-admin  
 vdc-admin

## Command History

Release	Modification
6.2(2)	This command was introduced.

## Usage Guidelines

M1 and M2 Series modules support exception SPAN only in the nonadministration virtual device context (VDC), and at least one interface of the module must be present for the VDC.

This command does not require a license.

## Examples

This example shows how to configure the source as an exception SPAN session:

```
switch(config)# monitor session 1
switch(config-monitor)# source exception all
```

This example shows how to configure the source as an exception ERSPAN session:

```
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# source exception all
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>monitor session</b>	Enters the monitor configuration mode.
<b>show monitor session</b>	Displays the virtual SPAN or ERSPAN configuration.



# switchport monitor

To configure the switchport interface as a Switched Port Analyzer (SPAN) destination, use the **switchport monitor** command. To disable the configuration, use the **no** form of this command.

**switchport monitor** [**ingress** [**learning**]]

**no switchport monitor** [**ingress** [**learning**]]

Syntax Description		
<b>ingress</b>	(Optional) Allows the SPAN destination port to inject packets that disrupt a certain TCP packet stream, for example, in networks with an intrusion detection system (IDS).	
<b>learning</b>	(Optional) Allows the SPAN destination port to inject packets, and allows the learning of MAC addresses, for example, the IDS MAC address.	

**Defaults** None

**Command Modes** Interface configuration mode

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to configure the Ethernet interface *7/2* as a SPAN destination:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface eth 7/2
switch(config-if)# switchport monitor
switch(config-if)#
```

This example shows how to configure the Ethernet interface *7/2* as a SPAN destination and allow it to inject packets and learn MAC addresses:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface eth 7/2
switch(config-if)# switchport monitor ingress learning
switch(config-if)#
```

This example shows how to disable the SPAN destination on Ethernet interface *7/2*:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface eth 7/2
switch(config-if)# no switchport monitor
```

## ■ switchport monitor

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>monitor session</b>	Enters the monitor configuration mode for configuring a SPAN session.
<b>show monitor session</b>	Displays the SPAN or ERSPAN session configuration.

# switchport monitor exclude header

To remove the FabricPath and VLAN tag headers for the specified SPAN destination ports in the VDC, use the **switchport monitor exclude header** command. To disable the configuration, use the **no** form of this command.

**switchport monitor exclude header**

**no switchport monitor exclude header**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Interface configuration mode

## Command History

Release	Modification
6.2(10)	This command was introduced.

## Usage Guidelines

This command does not require a license.

When you enter both the global and port-level configurations for this feature, the port-level overrides the global configuration.

## Examples

This example shows how to configure the Ethernet interface 7/2 to remove the FabricPath and VLAN tag headers to SPAN destination ports:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface eth 7/2
switch(config-if)# switchport monitor exclude header
switch(config-if)#
```

## Related Commands

Command	Description
<b>show running-config</b>	Displays the configuration for removing the FabricPath and VLAN tag headers from specified SPAN destination ports.

# system cores

To configure the destination for the system core, use the **system cores** command. To revert to the default, use the **no** form of this command.

```
system cores {slot0: [path] | tftp:/server// [path/]} filename
```

```
no system cores
```

## Syntax Description

<b>slot0:</b>	Specifies the slot0: external file system.
<i>path</i>	(Optional) Directory path to the file. The directory names in the path are case sensitive.
<b>tftp:</b>	Specifies a TFTP server.
<i>server</i>	Name or IPv4 address of the TFTP server. The server name is case sensitive.
<i>filename</i>	Name for the core file. The name is alphanumeric, case sensitive, and has a maximum of 32 characters.

## Defaults

None

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to configure a core file:

```
switch# configure terminal  
switch(config)# system cores slot0:core_file
```

This example shows how to disable system core logging:

```
switch# configure terminal  
switch(config)# no system cores
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	clear system cores	Clears the core file.
	show system cores	Displays the core filename.

# system default switchport monitor exclude header

To remove the FabricPath and VLAN tag headers for all SPAN destination ports in the VDC, use the **system default switchport monitor exclude header** command. To disable the configuration, use the **no** form of this command.

**system default switchport monitor exclude header**

**no system default switchport monitor exclude header**

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

**Defaults** None

**Command Modes** Global configuration mode

Command History	Release	Modification
	6.2(10)	This command was introduced.

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

**Examples** This example shows how to configure all SPAN destination ports to remove the FabricPath and VLAN tag headers:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# system default switchport monitor exclude header
switch(config)#
```

Related Commands	Command	Description
	<b>show running-config</b>	Displays the configuration for removing the FabricPath and VLAN tag headers from all SPAN destination ports.

# system hap-reset

To enable the Supervisor Reset high availability (HA) policy, use the **system hap-reset** command.

**system hap-reset**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to enable the Supervisor Reset HA policy:

```
switch(config)# system hap-reset
switch(config)#
```

Related Commands	Command	Description
	<b>show system standby manual-boot</b>	Displays the status of the system standby manual boot option.

# system heartbeat

To enable heartbeat checks (default) and revert to the factory default, use the **system heartbeat** command.

## system heartbeat

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to enable the heartbeat checks (default) and revert to the factory default:

```
switch(config)# system heartbeat
switch(config)#
```

Related Commands	Command	Description
	<b>system no hap-reset</b>	Disables the heartbeat checks (default) and reverts to the factory default.



# system mode maintenance

To put the switch in maintenance mode, use the **system mode maintenance** command. To exit the maintenance mode and return to normal mode, use the **no** form of the command.

**system mode maintenance**

**no system mode maintenance**

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

**Defaults** None

**Command Modes** Global configuration (config)

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

Command History	Release	Modification
	8.0(1)	This command has been enhanced to execute a normal mode profile and activate a timer ensuring that sufficient time is provided for the switch to complete any hardware programming that may be going on before the after_maintenance snapshot is taken.
	7.3(0)D1(1)	This command was modified. The default mode for Graceful Insertion and Removal (GIR) is "isolate".
	7.2(0)D1(1)	This command was introduced. The default mode for GIR is "shutdown".

**Usage Guidelines** In Cisco NX-OS Release 7.2(0)D1(1), the default mode for Graceful Insertion and Removal (GIR) is "shutdown". The switch will use the **shutdown** command to bring down the protocols and shut down the physical ports.

Starting with Cisco NX-OS Release 7.3(0)D1(1), the default mode for GIR is "isolate". The switch will use the **isolate** command to isolate the protocols from the network. The switch will then be isolated from the network but is not shut down.

Starting with Cisco NX-OS release 8.0(1), the [no] system mode maintenance command has been enhanced to execute a normal mode profile and activate a timer ensuring that sufficient time is provided for the switch to complete any hardware programming that may be going on before the after\_maintenance snapshot is taken. Once the timer expires, the after\_maintenance snapshot is taken in the background and a new warning syslog message, MODE\_SNAPSHOT\_DONE, is sent after the snapshot is complete. The default delay timer value is 120 seconds. The output of the [no] system

mode maintenance command displays the delay timer value, in seconds, after which the after\_maintenance snapshot is generated:

The after\_maintenance snapshot will be generated in <delay> seconds. After that time, please use 'show snapshots compare before\_maintenance after\_maintenance' to check the health of the system.

Starting with Cisco NX-OS Release 8.0(1), a visible CLI indicator has been added to show that the system is in maintenance mode. For example, switch(config)# will appear as switch(maint-mode)(config)#.

This command does not require a license

## Examples

This example shows how to put the switch in maintenance mode:

```
switch# configure terminal
switch(config)# system mode maintenance
Following configuration will be applied:
```

```
router bgp 100
  isolate
router ospf 100
  isolate
router isis 100
  isolate
```

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

```
Applying : router bgp 100
Applying :   isolate
Applying : router ospf 100
Applying :   isolate
Applying : router isis 100
Applying :   isolate
```

Maintenance mode operation successful.

This example shows how to put a switch, running the Cisco NX-OS Release 8.0(1), in maintenance mode:

```
switch# configure terminal
switch(config)# system mode maintenance
Following configuration will be applied:
```

```
router bgp 100
  isolate
router ospf 100
  isolate
router isis 100
  isolate
```

Do you want to continue (yes/no)? [no] y

Generating before\_maintenance snapshot before going into maintenance mode

Starting to apply commands...

```
Applying : router bgp 100
Applying :   isolate
Applying : router ospf 100
Applying :   isolate
Applying : router isis 100
```

```
Applying : isolate
```

```
Maintenance mode operation successful.  
switch(maint-mode)(config)# 2016 Dec 5 06:19:13 switch %$ VDC-1 %$ %  
MMODE-2-MODE_CHANGED: System changed to "maintenance" mode.
```

This example shows how to exit the maintenance mode and return to normal mode:

```
switch# configure terminal  
switch(config)# no system mode maintenance
```

Following configuration will be applied:

```
router isis 100  
  no isolate  
router ospf 100  
  no isolate  
router bgp 100  
  no isolate
```

```
Do you want to continue (y/n)? [no] y
```

```
Starting to apply commands...
```

```
Applying : router isis 100  
Applying : no isolate  
Applying : router ospf 100  
Applying : no isolate  
Applying : router bgp 100  
Applying : no isolate
```

```
Maintenance mode operation successful.
```

```
Generating Current Snapshot
```

```
Please use 'show snapshots compare before_maintenance after_maintenance' to check the  
health of the system
```

This example shows how to exit the maintenance mode and return to normal mode on a switch running the Cisco NX-OS Release 8.0(1):

```
switch# configure terminal  
switch(config)# no system mode maintenance
```

Following configuration will be applied:

```
router isis 100  
  no isolate  
router ospf 100  
  no isolate  
router bgp 100  
  no isolate
```

```
Do you want to continue (y/n)? [no] y
```

```
Starting to apply commands...
```

```
Applying : router isis 100  
Applying : no isolate  
Applying : router ospf 100  
Applying : no isolate  
Applying : router bgp 100  
Applying : no isolate
```

Maintenance mode operation successful.

The after\_maintenance snapshot will be generated in 120 seconds

After that time, please use 'show snapshots compare before\_maintenance after\_maintenance' to check the health of the system

```
switch(config)# 2016 Dec 5 06:20:23 switch %$ VDC-1 %$ %MMODE-2-MODE_CHANGED: System
changed to"normal" mode.
```

Related Commands	Command	Description
	<b>configure maintenance profile</b>	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
	<b>show system mode</b>	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
	<b>system mode maintenance always-use-custom-profile</b>	Applies the existing custom maintenance mode profile and prevents creation of auto-generated maintenance mode profile.
	<b>system mode maintenance on-reload reset-reason</b>	Boots the switch into maintenance mode automatically in the event of a specified system crash.
	<b>system mode maintenance shutdown</b>	Shuts down all protocols and interfaces except the management interface (by using the <b>shutdown</b> command and not the default <b>isolate</b> command).
	<b>system mode maintenance timeout</b>	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

# system mode maintenance always-use-custom-profile

To apply the existing custom maintenance-mode profile and prevent creation of auto-generated maintenance-mode profile, use the **system mode maintenance always-use-custom-profile** command.

**system mode maintenance always-use-custom-profile**

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

**Defaults** None

**Command Modes** Global configuration mode (config)

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

**Usage Guidelines** The **always-use-custom-profile** option forces the **dont-generate-profile** option to be used even if it has not been specified using the **system mode maintenance** command. You cannot use the "shutdown" option when the **always-use-custom-profile** option is being used.

This command does not require a license.

**Examples** This example shows how to always apply the existing custom maintenance mode profile and prevent creation of auto-generated maintenance mode profile:

```
switch(config)# system mode maintenance always-use-custom-profile
```

Related Commands	Command	Description
	<b>configure maintenance profile</b>	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
	<b>show run mmode</b>	Displays the currently running maintenance profile configuration on a switch.
	<b>show system mode</b>	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.

Command	Description
<b>system mode maintenance on-reload reset-reason</b>	Boots the switch into maintenance mode automatically in the event of a specified system crash.
<b>system mode maintenance shutdown</b>	Shuts down all protocols and interfaces except the management interface (by using the <b>shutdown</b> command and not the default <b>isolate</b> command).
<b>system mode maintenance timeout</b>	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

# system mode maintenance dont-generate-profile

To prevent the dynamic searching of enabled protocols and put the switch in maintenance mode by executing commands configured in a custom maintenance mode profile, use the **system mode maintenance dont-generate-profile** command. To exit maintenance mode and return to normal mode, use the **no** form of this command.

**system mode maintenance dont-generate-profile**

**no system mode maintenance dont-generate-profile**

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

**Defaults** None

**Command Modes** Global configuration (config)

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to prevent the dynamic searching of enabled protocols and put the switch in maintenance mode by executing commands configured in a custom maintenance mode profile:

```
switch(config)# system mode maintenance dont-generate-profile
```

Following configuration will be applied:

```
router bgp 100
  isolate
sleep instance 1 10
interface Ethernet1/1
  shutdown
```

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

## system mode maintenance dont-generate-profile

```
Starting to apply commands...

Applying : router bgp 100
Applying : isolate
Applying : sleep instance 1 10
Applying : interface Ethernet1/1
Applying : shutdown

Maintenance mode operation successful.
```

Related Commands	Command	Description
	<b>configure maintenance profile</b>	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
	<b>show run mmode</b>	Displays the currently running maintenance profile configuration on a switch.
	<b>show system mode</b>	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
	<b>system mode maintenance on-reload reset-reason</b>	Boots the switch into maintenance mode automatically in the event of a specified system crash.
	<b>system mode maintenance shutdown</b>	Shuts down all protocols and interfaces except the management interface (by using the <b>shutdown</b> command and not the default <b>isolate</b> command).
	<b>system mode maintenance timeout</b>	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.



# system mode maintenance non-interactive

To put the switch in maintenance mode without presenting any switch prompts, use the **system mode maintenance non-interactive** command. To return to normal mode from maintenance mode without presenting any switch prompts, use the **no** form of this command.

**system mode maintenance non-interactive**

**no system mode maintenance non-interactive**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Global configuration (config)

## Supported User Roles

network-admin  
vdc-admin  
network-operator  
vdc-operator

## Command History

Release	Modification
8.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to put the switch in maintenance mode without presenting any switch prompts:

```
switch(config)# system mode maintenance non-interactive
System mode switch to maintenance mode started. Will continue in background.
switch(config)# 2016 Dec 5 08:46:42 switch %$ VDC-1 %$ %MMODE-2-
MODE_CHANGED: System changed to "maintenance" mode.
switch(maint-mode)(config)#..
```

This example shows how to put the switch in normal mode from maintenance mode without presenting any switch prompts:

```
switch(config)# no system mode maintenance non-interactive
System mode switch to normal mode started. Will continue in background.
switch(maint-mode)(config)# 2016 Dec 5 08:48:01 switch %$ VDC-1 %$ %
MMODE-2-MODE_CHANGED: System changed to "normal" mode.
switch(config)#
```

Related Commands	Command	Description
	<b>configure maintenance profile</b>	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
	<b>show run mmode</b>	Displays the currently running maintenance profile configuration on a switch.
	<b>show system mode</b>	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.

# system mode maintenance on-reload reset-reason

To boot the switch into maintenance-mode automatically in the event of a specified system crash, use the **system mode maintenance on-reload reset-reason** command. To prevent the switch from being brought up in maintenance mode in the event of a system crash, use the **no** form of this command.

**system mode maintenance on-reload reset-reason** *reason*

**no system mode maintenance on-reload reset-reason** *reason*

## Syntax Description

<i>reason</i>	Specifies the reset reason. The reset reasons are as follows: <ul style="list-style-type: none"> <li>HW_ERROR—Hardware error</li> <li>SVC_FAILURE—Critical service failure</li> <li>KERN_FAILURE—Kernel panic</li> <li>WDOG_TIMEOUT—Watchdog timeout</li> <li>FATAL_ERROR—Fatal error</li> <li>MANUAL_RELOAD---Manual reload</li> <li>MAINTENANCE—Reloads the switch in maintenance mode if the switch was already in maintenance mode before reload.</li> <li>MATCH_ANY—Any of the above reasons</li> <li>ANY_OTHER—Any reload reason not specified above</li> </ul>
---------------	---

## Defaults

None

## Command Modes

Global configuration (config)

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

## Usage Guidelines

We recommend configuring the reset reason and saving it to the startup configuration. This enables the switch to go into the maintenance mode after a switch reloads due to any reason.

This command does not require a license.

**Examples**

This example shows how to automatically boot the switch into maintenance mode if a fatal error or a hardware error occurs

```
switch(config)# system mode maintenance on-reload reset-reason fatal_error
switch(config)# system mode maintenance on-reload reset-reason hw_error
```

**Related Commands**

Command	Description
<b>configure maintenance profile</b>	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
<b>show run mmode</b>	Displays the currently running maintenance profile configuration on a switch.
<b>show system mode</b>	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
<b>system mode maintenance shutdown</b>	Shuts down all protocols and interfaces except the management interface (by using the <b>shutdown</b> command and not the default <b>isolate</b> command).
<b>system mode maintenance timeout</b>	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

# system mode maintenance shutdown

To shut down all protocols and interfaces except the management interface (by using the **shutdown** command and not the default **isolate** command), use the **system mode maintenance shutdown** command.

## system mode maintenance shutdown

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

**Defaults** None

**Command Modes** Global configuration (config)

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

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

**Examples** This example shows how to shut down all protocol and interfaces on the switch except the management interface:

```
switch# configure terminal
switch(config)# system mode maintenance shutdown
```

Following configuration will be applied:

```
router bgp 100
  shutdown
router ospf 100
  shutdown
router isis 100
  shutdown
system interface shutdown
```

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

```

Applying : router bgp 100
Applying :  shutdown
Applying : router ospf 100
Applying :  shutdown
Applying : router isis 100
Applying :  shutdown
Applying : system interface shutdown

Maintenance mode operation successful.

```

Related Commands	Command	Description
	<b>configure maintenance profile</b>	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
	<b>show run mmode</b>	Displays the currently running maintenance profile configuration on a switch.
	<b>show system mode</b>	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
	<b>system mode maintenance on-reload reset-reason</b>	Boots the switch into maintenance mode automatically in the event of a specified system crash.
	<b>system mode maintenance timeout</b>	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

# system mode maintenance snapshot-delay

To change the snapshot-delay timer value, use the **system mode maintenance snapshot-delay** command. To remove the configured timer value, use the **no** form of this command.

```
system mode maintenance snapshot-delay delay-in-seconds
```

```
no system mode maintenance snapshot-delay delay-in-seconds
```

## Syntax Description

<i>delay-in-seconds</i>	Snapshot-delay timer value, in seconds. The range is from 0 to 65535.
-------------------------	---

## Defaults

The default snapshot-delay timer value is 120 seconds.

## Command Modes

Global configuration (config)

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
8.0(1)	This command was introduced.

## Usage Guidelines

The **[no] system mode maintenance** command has been enhanced from the previous release to execute a normal mode profile and activate a timer ensuring that sufficient time is provided for the switch to complete any hardware programming that may be going on before the `after_maintenance` snapshot is taken. Once the timer expires, the `after_maintenance` snapshot is taken in the background and a new warning syslog message, `MODE_SNAPSHOT_DONE`, is sent after the snapshot is complete.

Use the **system mode maintenance snapshot-delay** *delay-in-seconds* command to change the snapshot-delay timer value.

This command does not require a license.

## Examples

This example shows how to change the snapshot-delay timer value:

```
switch(config)# system mode maintenance snapshot-delay 5000
The after_maintenance snapshot delay has been set to 5000 seconds.
```

This example shows how to remove the configured snapshot-delay timer value:

```
switch(config)# no system mode maintenance snapshot-delay 5000
Using default after_maintenance snapshot delay of 120 seconds.
```

Related Commands	Command	Description
	<b>configure maintenance profile</b>	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
	<b>show run mmode</b>	Displays the currently running maintenance profile configuration on a switch.
	<b>show system mode</b>	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.



# system mode maintenance timeout

To configure the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes, use the **system mode maintenance timeout** command. To remove the configured timer, use the **no** form of this command.

**system mode maintenance timeout** *value*

**no system mode maintenance timeout** *value*

## Syntax Description

<i>value</i>	Specifies the number of minutes for which the switch will be in maintenance mode. Range is from 5 to 65535 minutes.
--------------	---

## Defaults

None

## Command Modes

Global configuration (config)

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

## Usage Guidelines

We recommend setting the timeout value to at least 30 minutes. Once the configured time elapses, the switch returns to normal mode automatically.

This command does not require a license.

## Examples

This example shows how to keep the switch in maintenance mode for a specific number of minutes:

```
switch# configure terminal
switch(config)# system mode maintenance timeout 30
```

## Related Commands

<b>Command</b>	<b>Description</b>
<b>configure maintenance profile</b>	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
<b>show run mmode</b>	Displays the currently running maintenance profile configuration on a switch.
<b>show system mode</b>	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
<b>system mode maintenance on-reload reset-reason</b>	Boots the switch into maintenance mode automatically in the event of a specified system crash.

# system no hap-reset

To disable the Supervisor Reset high availability (HA) policy, use the **system no hap-reset** command.

**system no hap-reset**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to disable the Supervisor Reset HA policy:

```
switch(config)# system no hap-reset
switch(config)#
```

Related Commands	Command	Description
	<b>system hap-reset</b>	Enables the Supervisor Reset HA policy.

# system no heartbeat

To disable the heartbeat checking (default) and revert to the factory default, use the **system no heartbeat** command.

## system no heartbeat

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to disable the heartbeat checks (default) and revert to the factory default:

```
switch(config)# system no heartbeat
switch(config)#
```

Related Commands	Command	Description
	<b>system heartbeat</b>	Enables the heartbeat checks (default) and reverts to the factory default.

# system no standby manual-boot

To disable the system standby manual boot option, use the **system no standby manual-boot** command.

**system no standby manual-boot**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to disable the system standby manual boot option:

```
switch(config)# system no standby manual-boot
system standby manual-boot option disabled
switch(config)#
```

Related Commands	Command	Description
	<b>show system standby manual-boot</b>	Displays the status of the system standby manual boot option.

# system no watchdog

To disable the watchdog feature, use the **system no watchdog** command.

**system no watchdog**

---

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

---

**Defaults** None

---

**Command Modes** Any command mode

---

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

---

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

---



---

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

---

**Examples** This example shows how to disable the watchdog feature:

```
switch(config)# system no watchdog
switch(config)#
```

---

Related Commands	Command	Description
	<b>system no watchdog kgdb</b>	Prevents the system from entering the Linux KGDB debugger on a watchdog failure.

---

# system no watchdog kgdb

To prevent the system from entering the Linux KGDB debugger on a watchdog failure, use the **system no watchdog kgdb** command.

**system no watchdog kgdb**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to prevent the system from entering the Linux KGDB debugger on a watchdog failure:

```
switch(config)# system no watchdog kgdb
switch(config)#
```

Related Commands	Command	Description
	<b>system no watchdog</b>	Disables the watchdog feature.

# system pss shrink

To shrink Persistent Storage Service (PSS) files on the system, use the **system pss shrink** command.

**system pss shrink**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to shrink PSS files on the system:

```
switch(config)# system pss shrink
pss shrink completed
switch(config)
```

Related Commands	Command	Description
	<b>show system pss shrink status</b>	Displays the last PSS shrink status.



# system scale-limit monitor

To enable scale limit monitoring on a switch, use the **system scale-limit monitor** command. To disable scale limit monitoring, use the **no** form of this command

**system scale-limit monitor** *time-in-minutes*

**no system scale-limit monitor**

## Syntax Description

*time-in-minutes* Specifies the interval (in minutes) at which the scale limits are monitored. The range is from 5 minutes to 43200 minutes (30 days).

## Defaults

Scale-limit monitoring is disabled.

## Command Modes

Global configuration mode

## Supported User Roles

network-admin  
vdc-admin  
network-operator  
vdc-operator

## Command History

Release	Modification
7.2(1)D1(1)	This command was introduced.

## Usage Guidelines

You can use the **system scale-limit monitor** command to monitor the following 16 scale parameters:

- FEX server interfaces
- F1 HW entries
- Virtual Port Channels (vPCs)
- Fabric Extenders (FEXs)
- Edge ports
- Port channels
- Intermediate System-to-Intermediate System (IS-IS) adjacencies
- Bidirectional Forwarding Detection (BFD) sessions
- L2-mroutes
- M2 HW entries
- Core ports
- M1 HW entries

- FabricPath Switch IDs
- VLANs
- FabricPath Topologies
- F2/F2e HW entries

This command does not require a license.

---

### Examples

This example shows how to enable scale limit monitoring on a switch:

```
switch(config)# system scale-limit monitor 40
```

---

### Related Commands

Command	Description
<code>show system internal scale-parameters</code>	Displays the scale parameters.

# system standby manual-boot

To display the standby manual-boot status, use the **system standby manual-boot** command.

**system standby manual-boot**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the standby manual-boot status:

```
switch(config)# system standby manual-boot
system standby manual-boot option enabled
switch(config)#
```

Related Commands	Command	Description
	<b>system startup-config</b>	Initializes the startup configuration.
	<b>init</b>	

# system startup-config init

To initialize the startup configuration, use the **system startup-config init** command.

**system startup-config init**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to initialize the startup configuration:

```
switch(config)# system startup-config init
WARNING: This command is going to re-initialize the contents of the startup-conf
figuration.
Do you want to continue? (y/n) [y]
```

Related Commands	Command	Description
	<b>system startup-config unlock</b>	Releases the system startup-configuration lock.

# system startup-config unlock

To release a system startup-configuration lock, use the **system startup-config unlock** command.

**system startup-config unlock** *luck-id*

<b>Syntax Description</b>	<i>luck-id</i>	Startup-configuration lock ID. The range is from 0 to 65536.
---------------------------	----------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to release a system startup-configuration lock:  <pre>switch(config)# <b>system startup-config unlock</b> switch(config)#</pre>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>system startup-config init</b>	Initializes the startup configuration.

# system test-preupgrade running-ver

To test the running software version before an upgrade, use the **system test-preupgrade running-ver** command.

```
system test-preupgrade running-ver version-number target-ver target-number swid id impact
impact-number
```

## Syntax Description

<i>version-number</i>	Software version number currently running on the system.
<b>target-ver</b>	Specifies the target version of the software.
<i>target-number</i>	Target version.
<b>swid</b>	Specifies the software ID of the image running on a module: system or kickstart.
<i>id</i>	Software ID.
<b>impact</b>	Specifies the impact: 0 for hitless and 1 for hitful.
<i>impact-number</i>	Impact number.

## Defaults

None

## Command Modes

Any command mode

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to test the running software version before an upgrade:

```
switch(config)# system test-preupgrade running-ver 4.2<0.202> target-ver Update
swid 4.2.1 impact 0
```

System will be upgraded according to following table:

Module	Swid	Impact	Running-Version	New-Version	Upg-Required
6	4.2.1	hitless	4.2<0.202>	Update	
1					
9	4.2.1	hitless	4.2<0.202>	Update	
1					
11	4.2.1	hitless	4.2<0.202>	Update	

1

Final upgrade impact table:

```
Module      Impact
-----
      6      hitless
      9      hitless
     11      hitless
```

Message from services:

```
switch(config)#
```

### Related Commands

Command	Description
<b>system startup-config unlock</b>	Releases a system startup-configuration lock.
<b>system startup-config init</b>	Initializes the startup configuration.

# system switchover

To switch over to the standby supervisor, use the **system switchover** command.

**system switchover**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to switch over to the standby supervisor:

```
switch# system switchover
switch#
```

Related Commands	Command	Description
	<b>show system redundancy</b>	Displays the system redundancy status.



# system trace

To configure a system trace level, use the **system trace** command. To remove the system trace level configuration, use the **no** form of this command.

```
system trace bit-mask
```

```
no system trace [bit-mask]
```

<b>Syntax Description</b>	<i>bit-mask</i> Bit mask to use to change the trace level of the system.				
<b>Defaults</b>	None				
<b>Command Modes</b>	Global configuration mode (config)				
<b>Supported User Roles</b>	network-admin vdc-admin				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
<b>Usage Guidelines</b>	This command does not require a license.				
<b>Examples</b>	<p>This example shows how to configure a system trace level:</p> <pre>switch(config)# system trace switch(config)#</pre> <p>This example shows how to remove the system trace level configuration:</p> <pre>switch(config)# system no trace switch(config)#</pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>show cores</td> <td>Displays the system core files.</td> </tr> </tbody> </table>	Command	Description	show cores	Displays the system core files.
Command	Description				
show cores	Displays the system core files.				

# system watchdog

To enable watchdog checks, use the **system watchdog** command.

**system watchdog**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to enable watchdog checks:

```
switch(config)# system watchdog
switch(config)#
```

Related Commands	Command	Description
	<b>system no watchdog</b>	Disables the watchdog feature.
	<b>system no watchdog kgdb</b>	Prevents the system from entering the Linux KGDB debugger on a watchdog failure.

# system watchdog kgdb

To configure the system to enter the Linux KGDB debugger on a watchdog failure, use the **system watchdog kgdb** command.

**system watchdog kgdb**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to configure the system to enter the Linux KGDB debugger on a watchdog failure:

```
switch(config)# system watchdog kgdb
switch(config)#
```

Related Commands	Command	Description
	<b>system watchdog</b>	Enables the watchdog feature.
	<b>system no watchdog</b>	Disables the watchdog feature.





# Show Commands

---

This chapter describes the Cisco NX-OS system management **show** commands.

# show callhome

To display information about the Call Home application, use the **show callhome** command.

```
show callhome { destination-profile [profile profile_name] | last action status | last merge status
| merge status | pending | pending-diff | session status | status | transport-email |
user-def-cmds }
```

Syntax	Description
<b>destination-profile</b>	Displays the name of the destination profile.
<b>profile</b>	(Optional) Displays the default profile name.
<i>profile_name</i>	Name of the profile. The name can be the default profile name or the profiles that you created.
<b>last action status</b>	Displays the status of the last Cisco Fabric Services (CFS) commit/abort operation.
<b>last merge status</b>	Displays the status of the last CFS merge operation for Call Home.
<b>merge status</b>	Displays the status of the last CFS merge operation for Call Home.
<b>pending</b>	Displays the Call Home configuration changes in the pending CFS database.
<b>pending-diff</b>	Displays the differences between the pending and running Call Home configuration. These differences would reflect changes made during the current CFS configuration session.
<b>session status</b>	Displays the status of the last CFS commit/abort operation for the Call Home configuration.
<b>status</b>	Displays the CFS distribution state (enabled or disabled) for Call Home.
<b>transport-email</b>	Displays the Call Home e-mail transport configuration.
<b>user-def-cmds</b>	Displays the CLI commands configured for each Call Home alert group.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples**

This example shows how to display the status of the last CFS operation for the Call Home application:

```
switch# show callhome last action status
Last Action Time Stamp      : None
Last Action                 : None
Last Action Result         : None
Last Action Failure Reason  : none
```

This example shows how to display the Call Home destination profile named Noc101:

```
switch# show callhome destination-profile profile Noc101

Noc101 destination profile information
maximum message size:2500000
message format:XML
message-level:0
email addresses configured:

alert groups configured:
all
```

This example shows how to display the Call Home configuration:

```
switch# show callhome
callhome enabled
Callhome Information:
contact person name(sysContact):who@where
contact person's email:someone@noc.com
contact person's phone number:+1-408-555-9918
street addr:425 E Street, Anytown, CA 95999
site id:8
customer id:987654
contract id:456789
switch priority:7
duplicate message throttling : enabled
periodic inventory : enabled
periodic inventory time-period : 7 days
periodic inventory timeofday : 08:00 (HH:MM)
Distribution : Enabled
```

**Related Commands**

Command	Description
<b>callhome test</b>	Sends a test message to all configured destinations.
<b>callhome send</b>	Sends the specified Call Home test message to all configured destinations.
<b>callhome</b>	Places you into the CLI call Home configuration mode.
<b>show cfs status</b>	Displays the status of CFS distribution on the device as well as IP distribution information.
<b>show tech-support cfs</b>	Displays information about the CFS configuration required by technical support when resolving a CFS issue.
<b>show logging level cfs</b>	Displays the CFS logging configuration.

# show callhome transport

To display the transport-related configuration for Call Home, use the **show callhome transport** command.

## show callhome transport

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the transport-related configuration for Call Home:

```
switch(config)# show callhome transport
http vrf:default

from email addr:person@company.com
reply to email addr:person@company.com

smtp server:10.1.1.174
smtp server port:25
smtp server vrf:
smtp server priority:0

smtp server:64.72.101.213
smtp server port:25
smtp server vrf:default
smtp server priority:60

smtp server:172.21.34.193
smtp server port:25
smtp server vrf:default
smtp server priority:50
```



```
smtp server:192.0.2.1
smtp server port:33
smtp server vrf:Neo
smtp server priority:1

smtp server:192.0.2.10
smtp server port:25
smtp server vrf:default
smtp server priority:4

switch(config)#
```

**Related Commands**

Command	Description
<b>show callhome</b>	Displays the Call Home configuration.

# show cdp

To display the interfaces that have the Cisco Discovery Protocol (CDP) enabled, use the **show cdp** command.

```
show cdp {all | entry {all | name name} | global | interface interface-type | traffic interface
interface-type}
```

Syntax Description		
<b>all</b>		Displays all interfaces in the CDP database.
<b>entry</b>		Displays CDP entries in the database.
<b>name</b> <i>name</i>		Displays a specific CDP entry that matches a name.
<b>global</b>		Displays CDP global parameters.
<b>interface</b> <i>interface-type</i>		Displays CDP parameters for an interface.
<b>traffic</b> <i>interface-type</i>		Displays CDP traffic statistics.
	<i>interface-type</i>	Type of interface.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the interfaces that have CDP enabled:

```
switch(config)# show cdp all
mgmt0 is up
  CDP enabled on interface
  Refresh time is 60 seconds
  Hold time is 30 seconds
Ethernet7/1 is down
  CDP enabled on interface
  Refresh time is 60 seconds
  Hold time is 30 seconds
```

```
Ethernet7/2 is down
  CDP enabled on interface
  Refresh time is 60 seconds
  Hold time is 30 seconds
Ethernet7/3 is down
  CDP enabled on interface
  Refresh time is 60 seconds
  Hold time is 30 seconds
Ethernet7/4 is down
  CDP enabled on interface
  Refresh time is 60 seconds
  Hold time is 30 seconds
Ethernet7/5 is down
  CDP enabled on interface
  Refresh time is 60 seconds
--More--
```

**Related Commands**

Command	Description
<code>enable cdp</code>	Enables CDP on an interface.

# show cdp neighbors

To display the status of Cisco Discovery Protocol (CDP) neighbors, use the **show cdp neighbors** command.

```
show cdp neighbors [interface interface]
```

<b>Syntax Description</b>	<b>interface</b> (Optional) Displays CDP neighbors on an interface. <i>interface</i>
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>Supported User Roles</b>	network-admin network-operator vdc-admin vdc-operator
-----------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	<p>This example shows how to display the status of CDP neighbors:</p> <pre>switch(config)# show cdp neighbors Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge                   S - Switch, H - Host, I - IGMP, r - Repeater,                   V - VoIP-Phone, D - Remotely-Managed-Device,                   s - Supports-STP-Dispute  Device-ID          Local Intrfce Hldtme Capability Platform      Port ID Switch            mgmt0         163      S I          WS-C2960-24TC Fas0/21 switch(config)#</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cdp holdtime</b>	Configures the time that CDP holds onto neighbor information before refreshing it.

# show cfs application

To display information about applications that are currently enabled to use Cisco Fabric Services (CFS) distribution, use the **show cfs application** command.

**show cfs application** [*name application\_name*]

<b>Syntax Description</b>	<b>name</b> (Optional) Displays the name of a specific application. <i>application_name</i>
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.1(2)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display CFS information about applications that are currently enabled to use CFS distribution:

```
switch# show cfs application
```

```
-----
Application   Enabled   Scope
-----
ntp           No       Physical-fc-ip
stp           Yes      Physical-eth
vpc           Yes      Physical-eth
igmp         Yes      Physical-eth
l2fm         Yes      Physical-eth
role          No       Physical-fc-ip
radius        No       Physical-fc-ip
callhome     Yes      Physical-fc-ip
```

```
Total number of entries = 8
```

This example shows how to display CFS information about the Call Home application:

## ■ show cfs application

```
switch# show cfs application name callhome
```

```
Enabled       : Yes
Timeout       : 20s
Merge Capable : Yes
Scope         : Physical-fc-ip
Region        : 4
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show <i>application_name</i> session status</b>	Displays the CFS configuration session status for the application, including the last action, the result, and the reason if there was a failure.
<b>show cfs internal</b>	Displays information internal to CFS including memory statistics, event history, and so on.
<b>show cfs lock</b>	Displays all active CFS fabric locks.
<b>show cfs merge status name</b>	Displays the merge status for a given CFS application.
<b>show cfs peers</b>	Displays all the CFS peers in the physical fabric.
<b>show cfs regions</b>	Displays all the CFS applications with peers and region information.
<b>show cfs status</b>	Displays the status of CFS distribution on the device as well as IP distribution information.
<b>show tech-support cfs</b>	Displays information about the CFS configuration required by technical support when resolving a CFS issue.
<b>show logging level cfs</b>	Displays the CFS logging configuration.

# show cfs lock

To display information about locks that are currently in place for an application that uses Cisco Fabric Services (CFS) for distribution, use the **show cfs lock** command.

```
show cfs lock [name application_name]
```

<b>Syntax Description</b>	<b>name</b> (Optional) Displays the name of a specific application. <i>application_name</i>
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>Supported User Roles</b>	network-admin network-operator vdc-admin vdc-operator
-----------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.1(2)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display a lock that is currently in place for the Call Home application that uses CFS for distribution:

```
switch(config-callhome)# show cfs lock name callhome
```

```
Scope      : Physical-fc-ip
```

```
-----
Switch WWN          IP Address          User Name   User Type
-----
20:00:00:22:55:79:a4:c1 172.28.230.85      admin      CLI/SNMP v3
switch
```

```
Total number of entries = 10
```

Related Commands	Command	Description
	<b>show <i>application_name</i> session status</b>	Displays the CFS configuration session status for the application, including the last action, the result, and the reason if there was a failure.
	<b>show cfs application</b>	Displays information about applications that are currently enabled to use CFS distribution.
	<b>show cfs internal</b>	Displays information internal to CFS including memory statistics, event history, and so on.
	<b>show cfs merge status name</b>	Displays the merge status for a given CFS application.
	<b>show cfs peers</b>	Displays all the CFS peers in the physical fabric.
	<b>show cfs regions</b>	Displays all the CFS applications with peers and region information.
	<b>show cfs static</b>	Displays all CFS static peers with status.
	<b>show cfs status</b>	Displays the status of CFS distribution on the device as well as IP distribution information.
	<b>show tech-support cfs</b>	Displays information about the CFS configuration required by technical support when resolving a CFS issue.
	<b>show logging level cfs</b>	Displays the CFS logging configuration.



# show cfs merge status

To display the merge status for an application that uses Cisco Fabric Services (CFS) for distribution, use the **show cfs merge status** command.

```
show cfs merge status [name application_name]
```

<b>Syntax Description</b>	<b>name</b> (Optional) Displays the name of a specific application. <i>application_name</i>
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>Supported User Roles</b>	network-admin network-operator vdc-admin vdc-operator
-----------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.1(2)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display the current merge status for the Call Home application that uses CFS for distribution. In this example, the most recent merge for the Call Home application was successful.

```
switch(config-callhome)# show cfs merge status name callhome

Physical-fc-ip Merge Status: Success [ Wed Dec 17 16:34:26 2008 ]
Local Fabric
-----
Switch WWN                IP Address
-----
20:00:00:22:55:79:a4:c1 172.28.230.85           [Merge Master]
                           switch

Total number of switches = 10
```

Related Commands	Command	Description
	<b>show <i>application_name</i> session status</b>	Displays the CFS configuration session status for the application, including the last action, the result, and the reason if there was a failure.
	<b>show cfs application</b>	Displays information about applications that are currently enabled to use CFS distribution.
	<b>show cfs internal</b>	Displays information internal to CFS including memory statistics, event history, and so on.
	<b>show cfs lock</b>	Displays all active CFS fabric locks.
	<b>show cfs peers</b>	Displays all the CFS peers in the physical fabric.
	<b>show cfs regions</b>	Displays all the CFS applications with peers and region information.
	<b>show cfs static</b>	Displays all CFS static peers with status.
	<b>show cfs status</b>	Displays the status of CFS distribution on the device as well as IP distribution information.
	<b>show tech-support cfs</b>	Displays information about the CFS configuration required by technical support when resolving a CFS issue.
	<b>show logging level cfs</b>	Displays the CFS logging configuration.

# show cfs peers

To display all peers in the physical fabric, use the **show cfs peers** command.

```
show cfs peers [name application_name]
```

<b>Syntax Description</b>	<b>name</b> (Optional) Displays the name of a specific application. <i>application_name</i>
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.1(2)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display all peers in the physical fabric for the Call Home application:

```
switch(config-callhome)# show cfs peers name callhome
```

```
Scope      : Physical-fc-ip
```

```
-----  
Switch WWN          IP Address  
-----  
20:00:00:22:55:79:a4:c1 172.28.230.85          [Local]  
                        switch
```

```
Total number of entries = 1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show application_name session status</b>	Displays the CFS configuration session status for the application, including the last action, the result, and the reason if there was a failure.
	<b>show cfs application</b>	Displays information about applications that are currently enabled to use CFS distribution.

<b>Command</b>	<b>Description</b>
<b>show cfs internal</b>	Displays information internal to CFS including memory statistics, event history, and so on.
<b>show cfs lock</b>	Displays all active CFS fabric locks.
<b>show cfs merge status name</b>	Displays the merge status for a given CFS application.
<b>show cfs regions</b>	Displays all the CFS applications with peers and region information.
<b>show cfs static</b>	Displays all CFS static peers with status.
<b>show cfs status</b>	Displays the status of CFS distribution on the device as well as IP distribution information.
<b>show tech-support cfs</b>	Displays information about the CFS configuration required by technical support when resolving a CFS issue.
<b>show logging level cfs</b>	Displays the CFS logging configuration.

# show cfs regions

To display all Cisco Fabric Services (CFS) applications with peers and region information, use the **show cfs regions** command.

```
show cfs regions { name application_name | region region_id}
```

```
show cfs regions brief { name application_name | region region_id}
```

Syntax Description	name	(Optional) Displays peer and region information for a specified application. <i>application_name</i>
	region <i>region_id</i>	Displays peer and region information for a specified region ID. The range is from 1 to 200.
	brief	Displays configured regions and applications but does not display peers.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to display a brief version of all CFS regions:

```
switch# show cfs regions brief
```

```
-----
Region      Application  Enabled
-----
3           radius      yes
4           callhome    yes
```

This example shows how to display a specified CFS region:

```
switch# show cfs regions region 4
```

## ■ show cfs regions

```

Region-ID : 4
Application: callhome
Scope     : Physical-fc-ip
-----
Switch WWN          IP Address
-----
20:00:00:22:55:79:a4:c1 172.28.230.85           [Local]
                        switch

Total number of entries = 1

```

---

**Related Commands**

Command	Description
<b>show <i>application_name</i> session status</b>	Displays the CFS configuration session status for the application, including the last action, the result, and the reason if there was a failure.
<b>show cfs application</b>	Displays information about applications that are currently enabled to use CFS distribution.
<b>show cfs internal</b>	Displays information internal to CFS including memory statistics, event history, and so on.
<b>show cfs lock</b>	Displays all active CFS fabric locks.
<b>show cfs merge status name</b>	Displays the merge status for a given CFS application.
<b>show cfs peers</b>	Displays all the CFS peers in the physical fabric.
<b>show cfs static</b>	Displays all CFS static peers with status.
<b>show cfs status</b>	Displays the status of CFS distribution on the device as well as IP distribution information.
<b>show tech-support cfs</b>	Displays information about the CFS configuration required by technical support when resolving a CFS issue.
<b>show logging level cfs</b>	Displays the CFS logging configuration.

# show cfs status

To display the current state of Cisco Fabric Services (CFS), use the **show cfs status** command.

## show cfs status

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to display the current state of CFS:

```
switch# show cfs status
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
Distribution over Ethernet : Disabled
Total number of entries = 8
```

Related Commands	Command	Description
	<b>show application_name session status</b>	Displays the CFS configuration session status for the application, including the last action, the result, and the reason if there was a failure.
	<b>show cfs internal</b>	Displays information internal to CFS including memory statistics, event history, and so on.
	<b>show cfs lock</b>	Displays all active CFS fabric locks.
	<b>show cfs merge status name</b>	Displays the merge status for a given CFS application.

<b>Command</b>	<b>Description</b>
<b>show cfs peers</b>	Displays all the CFS peers in the physical fabric.
<b>show cfs regions</b>	Displays all the CFS applications with peers and region information.
<b>show logging level cfs</b>	Displays the CFS logging configuration.
<b>show tech-support cfs</b>	Displays information about the CFS configuration required by technical support when resolving a CFS issue.



# show checkpoint

To display the contents of the checkpoint file, use the **show checkpoint** command.

**show checkpoint** [*name*]

<b>Syntax Description</b>	<i>name</i>	(Optional) Name of the checkpoint file. The name can be any alphanumeric string up to 63 characters.
---------------------------	-------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-operator vdc-admin
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display the contents of the checkpoint file:

```
switch# show checkpoint stable
```

```
-----
Name: stable
version 4.0(2)
power redundancy-mode combined force
license grace-period
feature vrrp
feature tacacs+
feature ospf
feature pim
feature pim6
feature msdp
feature eigrp
feature rip
feature isis
feature pbr
feature private-vlan
feature port-security
feature interface-vlan
```

## show checkpoint

```

feature dot1x
feature hsrp
feature lacp
feature glbp

feature dhcp
feature cts
logging level port-security 5
logging level glbp 6
snmp-server context foo
snmp-server community <removed> group vdc-operator
snmp-server community <removed> group network-admin
snmp-server community <removed> group vdc-admin
role feature-group name X
role feature-group name x
role name x
    vlan policy deny
    vrf policy deny
        permit vrf x
        permit vrf X
role name X
username adminbackup password 5 $1$0ip/C5Ci$oOdx7oJS1BCFpNRmQK4na. role vdc-ope
rator
username adminbackup role network-operator
username admin password 5 $1$8GYeC4uW$4WfnImcvtAKI6Uet.ePD.1 role network-admin

```

### Related Commands

Command	Description
<b>clear checkpoint database</b>	Clears out all the checkpoint files.

# show configuration session

To show information about the configuration sessions, use the **show configuration session** command.

**show configuration session** [*name*] [*status*] [*summary*]

Syntax Description	
<i>name</i>	(Optional) Name of the configuration session, The name can be any case-sensitive, alphanumeric string up to 63 characters.
<b>status</b>	(Optional) Shows the status of the configuration sessions.
<b>summary</b>	(Optional) Displays the summary of the active configuration sessions.

**Defaults** Display information for all sessions

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display information about a configuration session. Each line represents a CLI command that Cisco NX-OS applies to the device when you commit the session.

```
switch# show configuration session myACLs
config session name myACLs
0001 ip access-list test1
0002 permit tcp any any
0003 statistics
```

This example shows how to display the status of a configuration session:

```
switch(config-s)# show configuration session status
Session Name      : myACLs
Last Action       : None
Last Action Status : Success
Last Action Reason : -NA-
Last Action Timestamp : 00:00:00 UTC Jan 01 1970
```

This example shows how to display a summary of the configuration sessions:

## ■ show configuration session

```

switch(config-s)# show configuration session summary
Name                Session Owner      Creation Time
-----
myACLS              admin              21:34:39 UTC Apr 27 2008
status              admin              00:53:23 UTC Apr 29 2008
a                   admin              01:47:30 UTC Apr 28 2008
myACLS              admin              00:56:46 UTC Apr 29 2008
Number of active configuration sessions = 4
switch(config-s)#

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show tech-support session-mgr</b>	Shows detailed information about the configuration sessions for troubleshooting purposes.

# show configuration session global-info

To display information about the global configuration session, use the **show configuration session global-info** command.

## show configuration session global-info

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display information about the global configuration session:

```
switch(config)# show configuration session global-info
Maximum number of sessions allowed      : 32
Maximum number of commands (all ssns)  : 102400
Current number of active sessions       : 0
Current number of commands (all ssns)  : 0
switch(config)#
```

Related Commands	Command	Description
	<b>show configuration session</b>	Displays information about the configuration sessions.
	<b>show tech-support session-mgr</b>	Displays detailed information about the configuration sessions for troubleshooting purposes.

# show cores

To display the system core files from the virtual device contexts (VDCs), use the **show cores** command.

```
show cores [vdc-all | {vdc [e-vdc2 | vdc-id | switch]}]
```

Syntax Description	
<b>vdc-all</b>	(Optional) Displays core dumps from all VDCs.
<b>vdc</b>	Displays all core dumps for the VDC.
<i>e-vdc2</i>	(Optional) VDC ID number of a nondefault VDC. The range is from 1 to 8.
<i>vdc-id</i>	(Optional) VDC ID number. The range is from 1 to 8.
<b>switch</b>	(Optional) Displays the process core files for VDC number 1.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	6.2(2)	The <b>switch</b> keyword was added.
	4.0(1)	This command was introduced.

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

**Examples** This example shows how to display the system core files:

```
switch(config)# show cores vdc-all
VDC No Module-num Instance-num Process-name PID Core-create-time
-----
1 10 1 xmlsa 32442 May 8 15:24
1 10 1 xmlsa 25163 May 9 06:04
1 10 1 xmlsa 21581 May 9 13:25
switch(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<code>show system core</code>	Displays information about transferring cores.

# show diagnostic bootup level

To display information about bootup diagnostics, use the **show diagnostic bootup level** command.

**show diagnostic bootup level**

---

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

---

**Defaults** None

---

**Command Modes** Any command mode

---

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

---

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

---



---

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

---

**Examples** This example shows how to display information about the bootup diagnostic level:

```
switch# show diagnostic bootup level
Current bootup diagnostic level: complete
switch#
```

---

Related Commands	Command	Description
	<b>diagnostic bootup level</b>	Configures the diagnostic bootup level.

---



# show diagnostic content module

To display information about the diagnostic test content for a module, use the **show diagnostic content module** command.

```
show diagnostic content module {all | module_number}
```

Syntax Description	
<i>module_number</i>	Diagnostic content module number. The range is from 1 to 10.
<b>all</b>	Displays the diagnostic content for all modules.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** Use the **show diagnostic content module** command to display information about the tests configured on the module and the repeat interval time.

**Examples** This example shows how to display information about the diagnostic test content for a module:

```
switch# show diagnostic content module 6
Module 6: Supervisor module-1X (Active)
Diagnostics test suite attributes:
B/C/* - Bypass bootup level test / Complete bootup level test / NA
P/*   - Per port test / NA
S/*   - Only applicable to standby unit / NA
D/N/* - Disruptive test / Non-disruptive test / NA
H/*   - Always enabled monitoring test / NA
F/*   - Fixed monitoring interval test / NA
X/*   - Not a health monitoring test / NA
E/*   - Sup to line card test / NA
L/*   - Exclusively run this test / NA
T/*   - Not an ondemand test / NA
A/I/* - Monitoring is active / Monitoring is inactive / NA
```

ID	Name	Attributes	Testing Interval (hh:mm:ss)
_____	_____	_____	_____

## show diagnostic content module

```

1) ManagementPortLoopback-----> C**D**X**T* -NA-
2) EOBCPortLoopback-----> C**D**X**T* -NA-
3) ASICRegisterCheck-----> ***N*****A 00:00:20
4) USB-----> C**N**X**T* -NA-
5) CryptoDevice-----> C**N**X**T* -NA-
6) NVRAM-----> ***N*****A 00:00:30
7) RealTimeClock-----> ***N*****A 00:05:00
8) PrimaryBootROM-----> ***N*****A 00:30:00
9) SecondaryBootROM-----> ***N*****A 00:30:00
10) CompactFlash-----> ***N*****A 00:30:00
11) ExternalCompactFlash-----> ***N*****A 00:30:00
12) PwrMgmtBus-----> ***N*****A 00:00:30
13) SpineControlBus-----> ***N*****A 00:00:30
14) SystemMgmtBus-----> ***N*****A 00:00:30
switch

```

## Related Commands

Command	Description
<b>diagnostic start</b>	Starts on-demand diagnostics.
<b>diagnostic stop</b>	Stops on-demand diagnostics.
<b>show diagnostic bootup level</b>	Displays information about bootup diagnostics.
<b>show diagnostic description module</b>	Displays the diagnostic description.
<b>show diagnostic events</b>	Displays diagnostic events by error and information event type.
<b>show diagnostic ondemand setting</b>	Displays information about on-demand diagnostics.
<b>show diagnostic results module <i>slot</i></b>	Displays information about the results of a diagnostic.
<b>show diagnostic simulation module <i>slot</i></b>	Displays information about a simulated diagnostic.
<b>show diagnostic status module <i>slot</i></b>	Displays test status for all tests on a module.
<b>show module</b>	Displays module information including online diagnostic test status.

# show diagnostic description module

To display information about a diagnostic test for a module, use the **show diagnostic description module** command.

**show diagnostic description module** *slot test* { *test-ID* | *test-name* | **all** }

Syntax Description		
<i>slot</i>		Diagnostic description slot number. The slot range is from 1 to 10.
<b>test</b>		(Optional) Displays the diagnostic test selection.
<i>test-ID</i>		(Optional) Test ID. The range is from 1 to 14.
<i>test-name</i>		(Optional) Test name. The test name can be any case-sensitive, alphanumeric string up to 32 characters.
<b>all</b>		(Optional) Displays the test description for all tests on all modules.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display a diagnostic description for a module:

```
switch# show diagnostic description module 6 test 1
ManagementPortLoopback :
    A bootup test that tests loopback on the management port of
    the module
```

Related Commands	Command	Description
	<b>show diagnostic content</b>	Displays diagnostic test names and test IDs.

## show diagnostic eem

To display diagnostic Embedded Event Manager (EEM) action level and the EEM policies, use the **show diagnostic eem** command.

```
show diagnostic eem {action [description] | policy module {module number | all}}
```

### Syntax Description

<b>action</b>	Displays the EEM action level.
<b>description</b>	Displays the EEM action description.
<b>policy module</b>	Displays the EEM policies configured for the module.
<i>module number</i>	Displays the module number of a specific module. The range is from 1 to 9.
<b>all</b>	Displays all modules.

# show diagnostic events

To display information about diagnostic events, use the **show diagnostic events** command.

**show diagnostic events [error | info]**

Syntax Description	error	(Optional) Displays diagnostics by error type.
	info	(Optional) Displays diagnostics by information type.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to display diagnostic events:

```
switch# show diagnostic events
1) Event:E_DEBUG, length:114, at 404616 usecs after Wed Jan 7 09:38:46 2009
   [104] Event_INFO: TestName->ASICRegisterCheck TestingType->helth monitoring module->
   9 Result->pass Reason->Success

2) Event:E_DEBUG, length:114, at 414835 usecs after Wed Jan 7 09:38:26 2009
   [104] Event_INFO: TestName->ASICRegisterCheck TestingType->helth monitoring module->
   9 Result->pass Reason->Success

3) Event:E_DEBUG, length:107, at 294482 usecs after Wed Jan 7 09:38:23 2009
   [104] Event_INFO: TestName->PwrMgmtBus TestingType->helth monitoring module->9 Resul
t->pass Reason->Success
```

This example shows how to display diagnostic events by information type:

```
switch# show diagnostic events info
1) Event:E_DEBUG, length:114, at 934712 usecs after Wed Jan 7 11:40:06 2009
```

## show diagnostic events

```
[104] Event_INFO: TestName->ASICRegisterCheck TestingType->helth monitoring module->
9 Result->pass Reason->Success
```

2) Event:E\_DEBUG, length:110, at 314512 usecs after Wed Jan 7 11:39:53 2009

```
[104] Event_INFO: TestName->SystemMgmtBus TestingType->helth monitoring module->9 Re
sult->pass Reason->Success
```

This example shows how to display diagnostic events by event type:

```
switch# show diagnostic events error
switch#
```

### Related Commands

Command	Description
<b>show diagnostic content</b>	Displays diagnostic test names and test IDs.

# show diagnostic ondemand setting

To display information about the on-demand diagnostic test for a module, use the **show diagnostic ondemand setting** command.

## show diagnostic ondemand setting

<b>Syntax Description</b>	<b>setting</b>	Configures the diagnostic on-demand setting.
<b>Defaults</b>	None	
<b>Command Modes</b>	Any command mode	
<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.
<b>Usage Guidelines</b>	This command does not require a license.	
<b>Examples</b>	This example shows how to display diagnostic on-demand information:  switch# <b>show diagnostic ondemand setting</b> Test iterations = 1 Action on test failure = continue until test failure limit reaches 1	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>diagnostic ondemand setting</b>	Configures the diagnostic on-demand setting.

# show diagnostic result

To display diagnostic test results for a module, use the **show diagnostic result** command.

**show diagnostic result module** { *slot* [**test** [*test-id* | *test-name*]] | **all** } [**detail**]

Syntax Description	
<i>slot</i>	Diagnostic result slot number. The module slot range is from 1 to 10.
<b>test</b>	(Optional) Displays the diagnostic test selection.
<i>test-id</i>	(Optional) Test ID. The range is from 1 to 14.
<i>test-name</i>	(Optional) Test name. The test name can be any case-sensitive, alphanumeric string up to 32 characters.
<b>all</b>	Displays the test result for all tests on all modules.
<b>detail</b>	(Optional) Displays the detailed result.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display a diagnostic test result:

```
switch# show diagnostic result module 6 test 6 detail

Current bootup diagnostic level: complete
Module 6: Supervisor module-1X (Active)
Diagnostic level at card bootup: complete
Test results: (. = Pass, F = Fail, I = Incomplete,
              U = Untested, A = Abort, E = Error disabled)

-----
6) NVRAM-----> .
Error code -----> DIAG TEST SUCCESS
                Total run count -----> 1574
                Last test execution time ----> Thu Jun 26 09:28:40 2008
                First test failure time ----> n/a
```



```
switch# Last test failure time -----> n/a
Last test pass time -----> Thu Jun 26 09:28:41 2008
Total failure count -----> 0
Consecutive failure count ----> 0
Last failure reason -----> No failures yet
```

# show diagnostic simulation

To display information about a simulated diagnostic for a module, use the **show diagnostic simulation** command.

**show diagnostic simulation module** *slot*

<b>Syntax Description</b>	<i>slot</i>	Diagnostic simulation slot number. The range is from 1 to 10.
---------------------------	-------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display information about simulated diagnostics:
-----------------	--

```
switch# show diagnostic simulation module 6
Card(6): Supervisor module-1X
```

```
-NA-
switch#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>diagnostic test simulation</b>	Sets a simulated test result for a diagnostic test.

# show diagnostic status

To display the test status for all tests, use the **show diagnostic status** command.

**show diagnostic status module *slot***

<b>Syntax Description</b>	<i>slot</i> Diagnostic status slot number. The range is from 1 to 10.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

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

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display information about the test status for all tests on a module:
-----------------	--

```
switch# show diagnostic status module 6
      <BU>-Bootup Diagnostics, <HM>-Health Monitoring Diagnostics
      <OD>-OnDemand Diagnostics, <SCH>-Scheduled Diagnostics
=====
Card:(6) Supervisor module-1X
=====
Current running test           Run by
      -NA-                     -NA-
Currently Enqueued Test       Run by
      -NA-                     -NA-
switch#
```

# show diff rollback-patch

To display the differences between the source and destination, use the **show diff rollback-patch** command.

```
show diff rollback-patch { checkpoint name | running-config | startup-config }
```

Syntax Description	Parameter	Description
	<b>checkpoint</b>	Displays the checkpoint name as the source configuration.
	<i>name</i>	Name of the checkpoint file. The name can be any alphanumeric string up to 63 characters.
	<b>running-config</b>	Displays the running configuration as the destination.
	<b>startup-config</b>	Displays the startup configuration as the destination.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.0(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 stable checkpoint file and the running configuration:

```
switch# show diff rollback-patch checkpoint stable running-config
switch#
```

Related Commands	Command	Description
	<b>show checkpoint</b>	Displays the contents of the checkpoint file.
	<b>rollback running checkpoint</b>	Implements a rollback for the configured checkpoint file.

# show environment

To display information about the hardware environment status, use the **show environment** command.

**show environment [clock | fan | power | temperature]**

Syntax Description	
<b>clock</b>	(Optional) Displays information about the clock environment.
<b>fan</b>	(Optional) Displays information about the fan environment.
<b>power</b>	(Optional) Displays information about the power environment.
<b>temperature</b>	(Optional) Displays information about the temperature environment.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
vdc-admin  
  
network-operator  
vdc-operator

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

**Usage Guidelines** You can use this command to display information about the status of the hardware on your device. This command does not require a license.

**Examples** This example shows how to display information about the hardware environment:

```
switch# show environment
```

```
Clock:
```

```
-----
Clock          Model          Hw          Status
-----
A              Clock Module   --         NotSupported/None
B              Clock Module   --         NotSupported/None
```

## show environment

## Fan:

Fan	Model	Hw	Status
Fan1 (sys_fan1)		0.0	Ok
Fan2 (sys_fan2)		0.0	Ok
Fan3 (fab_fan1)		0.0	Ok
Fan4 (fab_fan2)		0.0	Ok
Fan_in_PS1	--	--	Ok
Fan_in_PS2	--	--	Ok
Fan_in_PS3	--	--	Absent
Fan Air Filter : Absent			

## Temperature:

Module	Sensor	MajorThresh (Celsius)	MinorThres (Celsius)	CurTemp (Celsius)	Status
2	Crossbar (s5)	105	95	40	Ok
2	CTSdev1 (s6)	115	105	47	Ok
2	CTSdev2 (s7)	115	105	51	Ok
2	CTSdev3 (s8)	115	105	47	Ok
2	CTSdev4 (s9)	115	105	48	Ok
2	CTSdev5 (s10)	115	105	47	Ok
2	CTSdev7 (s12)	115	105	50	Ok
2	CTSdev8 (s13)	115	105	50	Ok
2	CTSdev9 (s14)	115	105	48	Ok
2	CTSdev10 (s15)	115	105	48	Ok
2	CTSdev11 (s16)	115	105	46	Ok
2	CTSdev12 (s17)	115	105	45	Ok
2	QEng1Sn1 (s18)	115	105	43	Ok
2	QEng1Sn2 (s19)	115	105	42	Ok
2	QEng1Sn3 (s20)	115	105	39	Ok
2	QEng1Sn4 (s21)	115	105	40	Ok
2	L2Lookup (s22)	115	105	43	Ok
2	L3Lookup (s23)	120	110	54	Ok

## Power Supply:

Voltage: 50 Volts

PS	Model	Power (Watts)	Power (Amp)	Status
1	N7K-AC-6.0KW	0.00	0.00	Ok
2	N7K-AC-6.0KW	6000.00	120.00	Ok
3	-----	0.00	0.00	Absent

Mod	Model	Power Requested (Watts)	Power Requested (Amp)	Power Allocated (Watts)	Power Allocated (Amp)	Status
2	N7K-M148GT-11	247.00	4.94	247.00	4.94	Powered-Up
6	N7K-SUP1	210.00	4.20	210.00	4.20	Powered-Up
Xb1	N7K-C7010-FAB-1	123.50	2.47	123.50	2.47	Powered-Up

```

Power Usage Summary:
-----
Power Supply redundancy mode:           Non-Redundant (combined)
Power Supply redundancy operational mode: Non-Redundant (combined)

Total Power Capacity                    6000.00 W

Power reserved for Supervisor(s)       420.00 W
Power reserved for Fan Module(s)       2184.00 W
Power reserved for Fabric Module(s)    300.00 W
Power currently used by Modules        247.00 W

-----
Total Power Available                   2849.00 W
-----
    
```

This example shows how to display information about the power environment:

```
switch# show environment power
```

```

Power Supply:
Voltage: 50 Volts
-----
PS  Model                Power      Power      Status
   (Watts)      (Amp)
-----
1   FIORANO              0.00       0.00       Ok
2   FIORANO             6000.00    120.00     Ok
3   -----              0.00       0.00       Absent

Mod Model                Power      Power      Power      Power      Status
   Requested Requested  Allocated Allocated
   (Watts)      (Amp)      (Watts)      (Amp)
-----
2   NURBURGRING         247.00     4.94       247.00     4.94       Powered-Up
6   CATALUNYA           210.00     4.20       210.00     4.20       Powered-Up
Xb1 Estoril             123.50     2.47       123.50     2.47       Powered-Up

Power Usage Summary:
-----
Power Supply redundancy mode:           Non-Redundant (combined)
Power Supply redundancy operational mode: Non-Redundant (combined)

Total Power Capacity                    6000.00 W

Power reserved for Supervisor(s)       420.00 W
Power reserved for Fan Module(s)       2184.00 W
Power reserved for Fabric Module(s)    300.00 W
Power currently used by Modules        247.00 W

-----
Total Power Available                   2849.00 W
-----
    
```

**Related Commands**

Command	Description
<b>power redundancy-mode</b>	Configures the power supply redundancy mode.

# show environment power

To display information about the power capacity and power distribution of the system, use the **show environment power** command.

**show environment power** [**ampere** | **detail**]

Syntax Description	ampere	(Optional) Displays information about the power capacity and power distribution in amperes.
	detail	(Optional) Displays detailed information about the power capacity and power distribution.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** By reading information from the power supply, the system displays the power consumption information. The actual power consumed by the system might be more than what is displayed. This command does not require a license.



**Examples**

This example shows how to display information about the power capacity and power distribution of the system:

```
switch(config) show environment power ampere
Power Supply:
Voltage: 50 Volts
Power
Supply      Model                Actual      Total      Status
              Output      Capacity
              (Ampere)    (Ampere)
-----
1          N7K-AC-6.0KW          29.40 A    120.00 A    Ok
2          N7K-AC-6.0KW           0.00 A     0.00 A     Ok
3          -----             0.00 A     0.00 A     Absent
4          -----             0.00 A     0.00 A     Absent

Module      Model                Actual      Power      Status
              Draw      Allocated
              (Ampere)  (Ampere)
-----
6          N7K-M108X2-12L        371.00 A    17.00 A    Powered-Up
7          N7K-M148GS-11         254.00 A     9.00 A    Powered-Up
8          N7K-M148GS-11L        247.00 A     8.00 A    Powered-Up
9          supervisor            N/A         4.20 A     Absent
10         N7K-SUP1              N/A         4.20 A     Powered-Up
Xb1       N7K-C7018-FAB-1       N/A         2.00 A     Powered-Up
Xb2       xbar                  N/A         2.00 A     Absent
Xb3       xbar                  N/A         2.00 A     Absent
Xb4       xbar                  N/A         2.00 A     Absent
Xb5       xbar                  N/A         2.00 A     Absent
fan1     N7K-C7018-FAN         4.34 A     14.72 A    Powered-Up
fan2     N7K-C7018-FAN         3.78 A     10.74 A    Powered-Up

N/A - Per module power not available

Power Usage Summary:
-----
Power Supply redundancy mode (configured)          Non-Redundant (combined)
Power Supply redundancy mode (operational)         Non-Redundant (combined)

Total Power Capacity (based on configured mode)    120.00 A
Total Power of all Inputs (cumulative)             120.00 A
Total Power Output (actual draw)                  29.40 A
Total Power Allocated (budget)                    77.00 A
Total Power Available for additional modules       42.14 A
switch(config)#
```

**Related Commands**

Command	Description
<b>show environment</b>	Displays information about the hardware environment status.
<b>show hardware capacity</b>	Displays information about the platform hardware resources currently utilized by the system.

# show event manager environment

To display the name and value of Embedded Event Manager (EEM) environment variables, use the **show event manager environment** command.

**show event manager environment** { *varname* | **all** }

Syntax Description		
	<i>varname</i>	(Optional) Displays information about the specified environment variable.
	<b>all</b>	(Optional) Displays information about all environment variables. This is the default.

**Defaults** If no argument or keyword is specified, information for all environment variables is displayed.

**Command Modes** Privileged EXEC

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display all of the EEM environment variables:

```
switch# show event manager environment all
```

# show event manager event-types

To display the Embedded Event Manager (EEM) event types, use the **show event manager event-types** command.

```
show event manager event-types [detail | event-type-name] [module module]
```

Syntax Description	detail	(Optional) Displays details of all event types.
	<i>event-type-name</i>	(Optional) Name of the event type.
	<b>module</b> <i>module</i>	(Optional) Displays the events defined for a specific module. The range is from 1 to 10.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the details of the EEM event types:

```
switch# show event manager event-types detail
switch#
```

# show event manager history events

To display the Embedded Event Manager (EEM) events that have been triggered, use the **show event manager history events** command.

**show event manager history events** [**detail**] [**maximum number**] [**severity severity**]

Syntax Description	detail	(Optional) Displays details of all event types.
	<b>maximum number</b>	(Optional) Specifies the maximum number of history events to display.
	<b>severity severity</b>	(Optional) Displays only those events that were of the specified severity.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the EEM history events that have been triggered that were of severity 7:

```
switch# show event manager history events severity 7
switch#
```

# show event manager policy

To display the registered Embedded Event Manager (EEM) policies, use the **show event manager policy** command.

**show event manager policy** [**detail**] [*policy-name* | **inactive**]

Syntax Description	detail	(Optional) Displays details of all policies.
	<i>policy-name</i>	(Optional) Name of the policy.
	<b>inactive</b>	(Optional) Displays only those policies that are inactive.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the EEM policies:

```
switch# show event manager policy
switch#
```

# show event manager policy active

To display the Embedded Event Manager (EEM) policies that are executing, use the **show event manager policy active** command in the privileged EXEC mode.

**show event manager policy active** [*class class-options* | **[detailed]** [**queue-type** [**applet**]]]

Syntax Description	
<b>class class-options</b>	(Optional) Specifies EEM class policy. Specify either one or all of the following for <i>class-options</i> : <ul style="list-style-type: none"> <li><i>class-letter</i>: The class letter assigned to EEM policy. Letters range from A to Z. Multiple class letters can be specified.</li> <li><b>default</b>: Specifies policies registered with default class.</li> <li><b>range class-letter-range</b>: Specifies the EEM policy class in a range. Multiple instances of <b>range class-letter-range</b> can be specified. The letters must be in upper case.</li> </ul>
<b>detailed</b>	(Optional) Displays the detailed content of EEM policy.
<b>queue-type</b>	(Optional) Displays the queue type of the EEM policy.
<b>applet</b>	(Optional) Displays the EEM applet policy.

**Defaults** None

**Command Modes** privileged EXEC

Command History	Release	Modification
	7.2(0)D1(1)	This command was introduced.

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

**Examples** The following is a sample output from the **show event manager policy active** command that includes the priority, scheduler node, and event type fields::

```
switch# show event manager policy active
no. job id  p s  status  time of event  event type  name
1      1      N A  wait    Wed Oct8 21:45:10 2008  syslog     continue.tcl
2      12609  N A  running Mon Oct29 20:49:42 2007  timer watchdog  loop.tcl
```

The table below describes the significant fields shown in the display:

Field	Description
no	Index number automatically assigned to the policy.
job id	Unique internal EEM scheduler job identification number
p	Priority of the policy. There are four priorities: <ul style="list-style-type: none"> <li>• L - Indicates that the policy is of low priority</li> <li>• H - Indicates that the policy is of high priority.</li> <li>• N - Indicates that the policy is of normal priority.</li> <li>• Z - Indicates that the policy is of least priority.</li> </ul>
s	Scheduler node of the policy. There are two nodes: <ul style="list-style-type: none"> <li>• A - Indicates that the scheduler node of this policy is active.</li> <li>• S - Indicates that the scheduler node of this policy is standby.</li> </ul>
status	Scheduling status for the policy. There are six possible status values: <ul style="list-style-type: none"> <li>• pend - Indicates that the policy is awaiting execution.</li> <li>• running - Indicates that the policy is executing.</li> <li>• exec - Indicates that the policy has completed executing and is awaiting scheduler cleanup tasks.</li> <li>• hold - Indicates that the policy is being held.</li> <li>• wait - Indicates that the policy is waiting for a new event.</li> <li>• continue - Indicates that the policy receives a new event and is ready to run.</li> </ul>
time of event	Date and time when the policy was queued for execution in the EEM server.
event type	Type of event.
name	Name of the EEM policy.

**Related Commands**

Command	Description
<b>show event manager</b>	Shows the event manager details of an EEM policy.

# show event manager policy pending

To display the Embedded Event Manager (EEM) policies that are pending for execution, use the **show event manager policy pending** command in the privileged EXEC mode.

```
show event manager policy pending [queue-type applet [detailed] | class class-options |
detailed]
```

Syntax Description	
<b>queue-type</b>	(Optional) Displays the queue type of the EEM policy.
<b>applet</b>	(Optional) Displays the EEM applet policy.
<b>detailed</b>	(Optional) Displays the detailed content of EEM policy.
<b>class class-options</b>	(Optional) Displays EEM class policy. Specify either one or all of the following for <i>class-options</i> : <ul style="list-style-type: none"> <li><i>class-letter</i>: The class letter assigned to EEM policy. Letters range from A to Z. Multiple class letters can be specified.</li> <li><b>default</b>: Specifies policies registered with default class.</li> <li><b>range class-letter-range</b>: Specifies the EEM policy class in a range. Multiple instances of <b>range class-letter-range</b> can be specified. The letters must be in upper case</li> </ul>

**Defaults** None

**Command Modes** privileged EXEC

Command History	Release	Modification
	7.2(0)D1(1)	This command was introduced.

**Usage Guidelines** Pending policies are policies that are pending execution in the EEM server execution queue. When an event is triggered, the policy that is registered to handle the event is queued for execution in the EEM server. Use the **show event manager policy pending** command to display the policies in this queue and to view their details.

**Examples** The following is a sample output from the **show event manager policy pending** command:

```
switch# show event manager policy pending
no. job id  p s  status      time of event      event type      name
1   12851  N A  pend      Mon Oct29  20:51:18 2007  timer watchdog  loop.tcl
2   12868  N A  pend      Mon Oct29  20:51:24 2007  timer watchdog  loop.tcl
3   12873  N A  pend      Mon Oct29  20:51:27 2007  timer watchdog  loop.tcl
4   12907  N A  pend      Mon Oct29  20:51:41 2007  timer watchdog  loop.tcl
5   13100  N A  pend      Mon Oct29  20:52:55 2007  timer watchdog  loop.tcl
```



The table below describes the significant fields shown in the display:

Field	Description
no	Index number automatically assigned to the policy.
job id	Unique internal EEM scheduler job identification number
p	Priority of the policy. There are four priorities: <ul style="list-style-type: none"> <li>• L - Indicates that the policy is of low priority</li> <li>• H - Indicates that the policy is of high priority.</li> <li>• N - Indicates that the policy is of normal priority.</li> <li>• Z - Indicates that the policy is of least priority.</li> </ul>
s	Scheduler node of the policy. There are two nodes: <ul style="list-style-type: none"> <li>• A - Indicates that the scheduler node of this policy is active.</li> <li>• S - Indicates that the scheduler node of this policy is standby.</li> </ul>
status	Scheduling status for the policy. There are six possible status values: <ul style="list-style-type: none"> <li>• pend - Indicates that the policy is awaiting execution.</li> <li>• running - Indicates that the policy is executing.</li> <li>• exec - Indicates that the policy has completed executing and is awaiting scheduler cleanup tasks.</li> <li>• hold - Indicates that the policy is being held</li> <li>• wait - Indicates that the policy is waiting for a new event.</li> <li>• continue - Indicates that the policy receives a new event and is ready to run.</li> </ul>
time of event	Date and time when the policy was queued for execution in the EEM server.
event type	Type of event.
name	Name of the EEM policy.

#### Related Commands

Command	Description
<b>show event manager</b>	Shows the event manager details of an EEM policy.

# show event manager policy internal

To display Embedded Event Manager (EEM) policies that are already registered, use the **show event manager policy internal** command in the privileged EXEC mode.

**show event manager policy internal** [*word*] [*inactive*]

Syntax Description	
<i>word</i>	(Optional) Displays detailed information about the specified policy.
<i>inactive</i>	(Optional) Lists the policies that are not active in the system.

**Defaults** If this command is invoked with no optional keywords, it displays all registered EEM system and user policies for all event types. The policies are displayed according to the time at which they were registered.

**Command Modes** privileged EXEC

Command History	Release	Modification
	7.2(0)D1(1)	This command was introduced.

**Examples** The following is a sample output from the **show event manager policy internal** command:

```
switch# show event manager policy internal

      Name : POLICY_ORDER_CHECK_1
      Policy Type : applet
      Policy Registration Time : Policy Not Registered

      Name : POLICY_ORDER_CHECK_11
      Policy Type : applet
      Policy Registration Time : Policy Not Registered

      Name : POLICY_ORDER_CHECK_111
      Policy Type : applet
      Policy Registration Time : Policy Not Registered

switch# show event manager policy internal POLICY_ORDER_CHECK_1
      Name : POLICY_ORDER_CHECK_1
      Policy Type : applet
      Policy Registration Time : Policy Not Registered
```

Related Commands	Command	Description
	<b>show event manager</b>	Shows the event manager details of an EEM policy.

# show event manager policy-state

To display the state of the named Embedded Event Manager (EEM) policy, use the **show event manager policy-state** command.

```
show event manager policy-state name [module module]
```

<b>Syntax Description</b>	<i>name</i>	Name of a policy to display its state.
	<b>module</b> <i>module</i>	(Optional) Displays the policy state defined for a specific module. The range is from 1 to 10.

**Defaults** None

**Command Modes** Any command mode

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

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

**Examples** This example shows how to display the state of an EEM policy:

```
switch# show event manager policy-state policy42  
switch#
```

# show event manager scheduler

To display the schedule of Embedded Event Manager (EEM) policies that are scheduled, use the **show event manager scheduler** command in the privileged EXEC mode.

## show event manager scheduler thread detailed

Syntax Description	thread	Displays the thread for the scheduler.
	detailed	Displays the detailed content of EEM policies.

**Defaults** None

**Command Modes** privileged EXEC

Command History	Release	Modification
	7.2(0)D1(1)	This command was introduced.

**Usage Guidelines** Use the **show event manager scheduler** command to show all the EEM execution threads from the scheduler perspective and the details of the running policies.

**Examples** The following is a sample output from the **show event manager scheduler thread** command:

```
switch# show event manager scheduler thread

1 Script threads service class default total: 1 running: 1 idle: 0
2 Script threads service class range A-D total: 3 running: 0 idle: 3
3 Applet threads service class default total: 32 running: 0 idle: 32
4 Applet threads service class W X total: 5 running: 0 idle: 5

switch# show event manager scheduler thread detailed

1 Script threads service class default total: 1 running: 1 idle: 0
1 job id: 1, pid: 215, name: continue.tcl
2 Script threads service class range A-D total: 3 running: 0 idle: 3
3 Applet threads service class default total: 32 running: 0 idle: 32
4 Applet threads service class W X total: 5 running: 0 idle: 5
```

Related Commands	Command	Description
	show event manager	Shows the event manager details of an EEM policy.

# show event manager script

To display the script policy of the Embedded Event Manager (EEM), use the **show event manager script** command.

**show event manager script system** {*name* | **all**}

## Syntax Description

<i>name</i>	Script name to display.
<b>all</b>	Displays all the system scripts.

## Defaults

None

## Command Modes

Any command mode

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to display all the system scripts defined in the EEM:

```
switch# show event manager script system all
switch#
```

# show event manager system-policy

To display the system policies of the Embedded Event Manager (EEM), use the **show event manager system-policy** command.

**show event manager system-policy [all]**

<b>Syntax Description</b>	<b>all</b>	(Optional) Displays all policies (including advanced policies and those policies that cannot be overridden).
---------------------------	------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples**

This example shows how to display the EEM system policies:

```
switch# show event manager system-policy
Name : __BootupPortLoopback
  Description : Do CallHome, log error on affected ports after 1 consecutive f
ailure of GOLD "BootupPortLoopback" test
  Overridable : Yes

      Name : __PortLoopback
  Description : Do CallHome, log error and disable further HM testing on affec
ted ports after 10 consecutive failures of GOLD "PortLoopback" test
  Overridable : Yes

      Name : __RewriteEngineLoopback
  Description : Do CallHome, log error and disable further HM testing on affec
ted ports after 10 consecutive failures of GOLD "RewriteEngineLoopback" test
  Overridable : Yes

      Name : __asic_register_check
  Description : Do CallHome, log error and disable further HM testing for that
ASIC device/instance after 20 consecutive failures of GOLD "AsicRegisterCheck"
test
  Overridable : Yes

      Name : __compact_flash
  Description : Do CallHome, log error and disable further HM testing after 20
consecutive failures of GOLD "CompactFlash" test
  Overridable : Yes

      Name : __crypto_device
  Description : Do CallHome and log error when GOLD "CryptoDevice" test fails
  Overridable : Yes

      Name : __eobc_port_loopback
  Description : Do CallHome and log error when GOLD "EOBCPortLoopback" test fa
ils
  Overridable : Yes

      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 : __external_compact_flash
  Description : Do CallHome, log error and disable further HM testing after 20
consecutive failures of GOLD "ExternalCompactFlash" test
  Overridable : Yes
switch#
```

# show flow exporter

To display the Flexible NetFlow flow exporter status and statistics, use the **show flow exporter** command.

**show flow exporter** [**name** *exporter-name*]

## Syntax Description

<b>name</b> <i>exporter-name</i>	(Optional) Specifies the name of a flow exporter. The name can be any case-sensitive, alphanumeric string up to 64 characters.
----------------------------------	--

## Defaults

Information for all flow exporters configured on the router is displayed.

## Command Modes

Any command mode

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

You must have already enabled traffic monitoring with Flexible NetFlow using an exporter before you can use the **show flow exporter** command.

This command does not require a license.

## Examples

This example shows how to display the status and statistics for all of the flow exporters configured on the router:

```
switch# show flow exporter
Flow Exporter NFC-DC-PHOENIX:
Export Version 5
Exporter Statistics
  Number of Flow Records Exported 0
  Number of Export Packets Sent 0
  Number of Export Bytes Sent 0
  Number of Destination Unreachable Events 0
  Number of No Buffer Events 0
  Number of Packets Dropped (No Route to Host) 0
  Number of Packets Dropped (other) 0
  Number of Packets Dropped (LC to RP Error) 0
  Number of Packets Dropped (Output Drops) 0
  Time statistics were last cleared: Never
Flow exporter timeout:
```



```

Export Version 5
Exporter Statistics
  Number of Flow Records Exported 0
  Number of Export Packets Sent 0
  Number of Export Bytes Sent 0
  Number of Destination Unreachable Events 0
  Number of No Buffer Events 0
  Number of Packets Dropped (No Route to Host) 0
  Number of Packets Dropped (other) 0
  Number of Packets Dropped (LC to RP Error) 0
  Number of Packets Dropped (Output Drops) 0
  Time statistics were last cleared: Never
Flow exporter test-exporter:
  Description: test server in San Jose CA
  Export Version 5
  Exporter Statistics
    Number of Flow Records Exported 0
    Number of Export Packets Sent 0
    Number of Export Bytes Sent 0
    Number of Destination Unreachable Events 0
    Number of No Buffer Events 0
    Number of Packets Dropped (No Route to Host) 0
    Number of Packets Dropped (other) 0
    Number of Packets Dropped (LC to RP Error) 0
    Number of Packets Dropped (Output Drops) 0
    Time statistics were last cleared: Never

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear flow exporter</b>	Clears the statistics for exporters.
<b>destination</b>	Configures an export destination for flow exporters.
<b>dscp</b>	Configures optional differentiated services code point (DSCP) parameters for flow exporters.
<b>export-protocol</b>	Configures the export protocol version for flow exporters.
<b>flow exporter</b>	Creates a flow exporter.
<b>option</b>	Configure options for flow exporters.
<b>show flow exporter</b>	Displays flow exporter status and statistics.
<b>source</b>	Configures the source IP address interface for flow exporters.
<b>template</b>	Configures the template resend timeout for flow exporters.
<b>transport</b>	Configures the transport protocol for flow exporters.
<b>tll</b>	Configures the time-to-live (TTL) value for flow exporters.

# show flow interface

To display the Flexible NetFlow configuration and status for an interface, use the **show flow interface** command.

```
show flow interface [interface-type number]
```

## Syntax Description

<i>interface-type number</i>	(Optional) Type of interface that you want to view Flexible NetFlow accounting configuration information on.
------------------------------	--

## Defaults

Information for the Flexible NetFlow accounting configuration on the interface is displayed.

## Command Modes

Any command mode

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

You must have already enabled traffic monitoring with Flexible NetFlow before you can use the **show flow interface** command.

This command does not require a license.

## Examples

This example shows how to display the Flexible NetFlow accounting configuration on interface Ethernet 0/0 and 0/1:

```
switch# show flow interface ethernet 1/0
Interface Ethernet1/0
  FNF:  monitor:      NFC-DC-PHOENIX
        direction:   Output
        traffic(ip):  on

switch# show flow interface ethernet 0/0
Interface Ethernet0/0
  FNF:  monitor:      FLOW-MONITOR-1
        direction:   Input
        traffic(ip):  sampler SAMPLER-2#
```

Table 1 describes the significant fields shown in the display.

**Table 1** *show flow interface Field Descriptions*

Field	Description
Interface	The interface that information is applicable to.
monitor	The name of the flow monitor that is configured on the interface.
direction:	The direction of traffic the flow monitor is monitoring. The possible values are as follows: <ul style="list-style-type: none"> <li>• Input—Traffic being received by the interface</li> <li>• Output—Traffic being transmitted by the interface</li> </ul>
traffic (ip)	Indicates if the flow monitor is in normal mode or sampler mode. The possible values are as follows: <ul style="list-style-type: none"> <li>• On—The flow monitor is in normal mode.</li> <li>• Sampler— The flow monitor is in sampler mode (the name of the sampler is included in the display).</li> </ul>

#### Related Commands

Command	Description
<b>show flow sw-monitor</b>	Displays flow monitor status and statistics.

# show flow monitor

To display the status and statistics for a Flexible NetFlow flow monitor, use the **show flow monitor** command.

**show flow monitor** [*name monitor-name*] [*cache*]

Syntax Description	
<b>name</b> <i>monitor-name</i>	(Optional) Specifies the name of a flow monitor that you configured by using the <b>flow monitor</b> command.
<b>cache</b>	(Optional) Displays the flow of packets generated by the supervisor. Use this command with the <b>show hardware flow {ip   ipv6}</b> command to get all the flows on the system.

**Defaults** Information for all flow exporters configured on the router is displayed.

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	6.2(10)	This command introduced. This command replaced the <b>show flow sw-monitor</b> command.

**Usage Guidelines** You must have already enabled traffic monitoring with Flexible NetFlow before you can use this command.

This command does not require a license.

**Examples** This example shows how to display the status and statistics for the flow monitor named mon\_IPv4:

```
switch# show flow monitor mon_IPv4 cache
```

SrcAddr	DstAddr	Dir	PktCnt	ByteCnt
10.1.1.1	10.1.1.2	Egr	246	16412
10.1.1.1	10.1.1.2	Egr	1	70
10.1.1.1	10.1.1.2	Egr	1	74
10.1.1.1	10.1.1.2	Egr	1	74
20.1.1.1	20.1.1.2	Egr	1	74

The following table describes the significant fields shown in the display.

**Table 2** *show flow monitor Field Descriptions*

Field	Description
SrcAddr	The source address.
DstAddr	The destination address.
PktCnt	The number of packets that have been counted.
ByteCnt	The number of bytes that have been counted.

#### Related Commands

Command	Description
<b>cache</b>	Configures flow cache parameters for flow monitors.
<b>clear flow monitor</b>	Clears the flow monitor.
<b>exporter</b>	Specifies a flow exporter for flow monitors.
<b>flow monitor</b>	Creates a flow monitor.
<b>protocol-distribution</b>	Configures the collection of protocol distribution statistics for flow monitors.
<b>record</b>	Configures a flow record for the flow monitor.
<b>show hardware flow</b>	Displays information about NetFlow hardware IP flows.
<b>size-distribution</b>	Configures the collection of size distribution statistics for flow monitors.

# show flow sw-monitor

To display the status and statistics for a Flexible NetFlow flow monitor, use the **show flow sw-monitor** command.

**show flow sw-monitor** [**name** *exporter-name*] [**cache** [**detailed**]]

Syntax Description	
<b>name</b> <i>exporter-name</i>	(Optional) Specifies the name of a flow exporter. The name can be any case-sensitive, alphanumeric string up to 64 characters.
<b>cache</b>	Displays the flow of packets generated by the supervisor. Use this command with the <b>show hardware flow {ip   ipv6}</b> command to get all the flows on the system.
<b>detailed</b>	(Optional) Displays detailed information about the flow of packets.

**Defaults** Information for all flow exporters configured on the router is displayed.

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	6.2(10)	This command has been deprecated. This command was replaced by the <b>show flow monitor</b> command.
	4.0(1)	This command was introduced.

**Usage Guidelines** You must have already enabled traffic monitoring with Flexible NetFlow using an exporter before you can use the **show flow exporter** command.

This command does not require a license.

**Examples** This example shows how to display the status and statistics for a flow monitor:

```
switch# show flow sw-monitor NFC-DC-PHOENIX statistics
Cache type:                               Normal
Cache size:                               4096
Current entries:                           4
High Watermark:                            6

Flows added:                               116
Flows aged:                                112
```

```

- Active timeout ( 1800 secs)      0
- Inactive timeout ( 15 secs)     112
- Event aged                       0
- Watermark aged                  0
- Emergency aged                  0

```

Table 3 describes the significant fields shown in the display.

**Table 3** *show flow sw-monitor monitor-name Field Descriptions*

Field	Description
Cache Type	The flow monitor cache type. The possible values are as follows: <ul style="list-style-type: none"> <li>• Normal—Flows are expired normally</li> <li>• Permanent—Flows are never expired</li> <li>• Immediate—Flows are expired immediately</li> </ul>
Cache Size	The number of entries in the cache.
Current entries	The number of entries in the cache that are in use.
High Watermark	The highest number of cache entries seen.
Flows added	Flows added to the cache since the cache was created.
Flows aged	Flows expired from the cache since the cache was created.
Active Timeout	The current value for the active timeout.
Inactive Timeout	The current value for the inactive timeout.
Event aged	The number of flows that have been aged by an event such as using the <b>force-export</b> option for the <b>clear flow monitor</b> command or the counter value wrapped because the maximum number for the counter was reached.
Watermark aged	The number of flows that have been aged because they exceeded the maximum high watermark value.
Emergency aged	The number of flows that were aged from the cache to allow new flows to be added.

This example shows how to display the status for a flow monitor:

```

switch# show flow sw-monitor NFC-DC-PHOENIX

Flow Monitor NFC-DC-PHOENIX:
  Description:      Used for basic traffic analysis
  Flow Record:     netflow-original
  Flow Exporter:   EXP-DC-TOPEKA
                  EXP-DC-PHOENIX

Cache:
  Type:            normal
  Status:         allocated
  Size:           4096 entries / 311316 bytes
  Inactive Timeout: 15 secs
  Active Timeout:  1800 secs
  Update Timeout:  1800 secs

```

Table 4 describes the significant fields shown in the display.

**Table 4** *show flow sw-monitor monitor-name Field Descriptions*

Field	Description
Flow Monitor	The name of the flow monitor that you configured.
Description	The description that you configured for the monitor, or the default description—User defined.
Flow Record	The flow record assigned to the flow monitor.
Flow Exporter	The exporter(s) that are assigned to the flow monitor.
Cache	Information on the cache for the flow monitor.
Type	The flow monitor cache type. The possible values are as follows: <ul style="list-style-type: none"> <li>• Normal—Flows are expired normally</li> <li>• Permanent—Flows are never expired</li> <li>• Immediate—Flows are expired immediately</li> </ul>
Status	The status of the flow monitor cache. The possible values are as follows: <ul style="list-style-type: none"> <li>• Allocated—The cache is allocated.</li> <li>• Being deleted—The cache is being deleted.</li> <li>• Not allocated—The cache is not allocated.</li> </ul>
Size	The current cache size.
Inactive Timeout	The current value for the inactive timeout.
Active Timeout	The current value for the active timeout.
Update Timeout	The current value for the update timeout.

This example shows how to display the status and statistics for the flow monitor named NFC-DC-PHOENIX:

```
switch# show flow sw-monitor NFC-DC-PHOENIX cache
Cache type:                               Normal
Cache size:                               4096
Current entries:                           8
High Watermark:                           10

Flows added:                              1560
Flows aged:                                1552
- Active timeout ( 1800 secs)              24
- Inactive timeout ( 15 secs)              1528
- Event aged                               0
- Watermark aged                           0
- Emergency aged                           0

IP TOS:                                    0x00
IP PROTOCOL:                               6
IPV4 SOURCE ADDRESS:                       10.10.10.2
IPV4 DESTINATION ADDRESS:                   172.16.10.2
TRNS SOURCE PORT:                           20
```



```

TRNS DESTINATION PORT:    20
INTERFACE INPUT:         Et0/0
FLOW SAMPLER ID:         0
ip source as:            0
ip destination as:       0
ipv4 next hop address:   172.16.7.2
ipv4 source mask:        /0
ipv4 destination mask:   /24
tcp flags:               0x00
interface output:        Et1/0
counter bytes:           198520
counter packets:         4963
timestamp first:         10564356
timestamp last:          12154104

```

Table 5 describes the significant fields shown in the display.

**Table 5** *show flow sw-monitor monitor-name Field Descriptions*

Field	Description
Cache type	The flow monitor cache type. The possible values are as follows: <ul style="list-style-type: none"> <li>• Normal—Flows are expired normally</li> <li>• Permanent—Flows are never expired</li> <li>• Immediate—Flows are expired immediately</li> </ul>
Cache Size	The number of entries in the cache.
Current entries	The number of entries in the cache that are in use.
High Watermark	The highest number of cache entries seen.
Flows added	Flows added to the cache since the cache was created.
Flows aged	Flows expired from the cache since the cache was created.
Active timeout	The current value for the inactive timeout.
Inactive timeout	The current value for the active timeout.
Event aged	The number of flows that have been aged by an event such as using the <b>force-export</b> option for the <b>clear flow monitor</b> command.
Watermark aged	The number of flows that have been aged because they exceeded the maximum high watermark value.
Emergency aged	The number of flows that were aged from the cache to allow new flows to be added.
IP TOS	The IP type of service (ToS) value.
IP PROTOCOL	The protocol number.
IPV4 SOURCE ADDRESS	The IPv4 source address.
IPV4 DESTINATION ADDRESS	The IPv4 destination address.
TRNS SOURCE PORT	The source port for the transport protocol.
TRNS DESTINATION PORT	The destination port for the transport protocol.
INTERFACE INPUT	The interface that the input is received on.
FLOW SAMPLER ID	The flow sampler ID number.

**Table 5** *show flow sw-monitor monitor-name Field Descriptions (continued)*

Field	Description
ip source as	The BGP source AS number.
ip destination as	The BGP destination AS number.
ipv4 next hop address	The IPv4 address of the next hop that the packet is forwarded to.
ipv4 source mask	The IPv4 source address mask.
ipv4 destination mask	The IPv4 destination address mask.
tcp flags	The value of the TCP flags.
interface output	The interface that the input is transmitted on.
counter bytes	The number of bytes that have been counted.
counter packets	The number of packets that have been counted.
timestamp first	The timestamp of the first packet in the flow.
timestamp last	The timestamp of the last packet in the flow.

This example shows how to display the status and statistics for the flow monitor named NFC-DC-PHOENIX in a table format:

```
switch# show flow sw-monitor NFC-DC-PHOENIX cache format table
Cache type:                               Normal
Cache size:                               4096
Current entries:                           4
High Watermark:                            6

Flows added:                               90
Flows aged:                                86
- Active timeout ( 1800 secs)              0
- Inactive timeout ( 15 secs)              86
- Event aged                               0
- Watermark aged                           0
- Emergency aged                           0

IP TOS   IP PROT   IPV4 SRC ADDR   IPV4 DST ADDR   TRNS SRC PORT   TRNS DST PORT
=====  =====  =====
0x00     1         10.251.10.1    172.16.10.2    0                02
0x00     1         10.251.10.1    172.16.10.2    0                20484
0xC0     17        172.16.6.1     224.0(1).0.9   520              5202
0x00     6         10.10.11.1     172.16.10.5    25               252
switch#
```

**Related Commands**

Command	Description
<b>cache</b>	Configures flow cache parameters for flow monitors.
<b>clear flow monitor</b>	Clears the flow monitor.
<b>exporter</b>	Specifies a flow exporter for flow monitors.
<b>flow monitor</b>	Creates a flow monitor.
<b>protocol-distribution</b>	Configures the collection of protocol distribution statistics for flow monitors.
<b>record</b>	Configures a flow record for the flow monitor.

<b>Command</b>	<b>Description</b>
<b>show flow sw-monitor</b>	Displays flow monitor status and statistics.
<b>size-distribution</b>	Configures the collection of size distribution statistics for flow monitors.

# show flow record

To display the status and statistics of a Flexible NetFlow flow record, use the **show flow record** command.

**show flow record** [**name** *record-name* | **netflow ipv4** *record* | **netflow-original**]

Syntax Description	
<b>name</b> <i>record-name</i>	(Optional) Specifies the name of a flow record that you previously configured.
<b>netflow ipv4</b> <i>record</i>	(Optional) Configures the flow monitor to use one of the predefined records. See <a href="#">Table 6</a> for a listing of the available records and their definitions.
<b>netflow-original</b>	(Optional) Specifies the Flexible NetFlow implementation of original NetFlow with origin autonomous systems.

**Defaults** Information for all flow exporters configured on the router is displayed.

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** You must have already enabled traffic monitoring with Flexible NetFlow using an exporter before you can use the **show flow exporter** command.

[Table 6](#) describes the keywords and descriptions for the *record* argument.

**Table 6** Keywords and Descriptions for the record Argument

<b>original-input</b>	Traditional IPv4 input NetFlow.
<b>original-output</b>	Traditional IPv4 output NetFlow.
<b>protocol-port</b>	Protocol ports record.

This command does not require a license.

**Examples** This example shows how to display the status and statistics of the original input NetFlow record:

```

switch# show flow record netflow ipv4 original-input
Flow record ipv4 original-input:
  Description: Traditional IPv4 input NetFlow
  No. of users: 0
  Template ID: 0
  Fields:
    match ipv4 source address
    match ipv4 destination address
    match ip protocol
    match ip tos
    match transport source-port
    match transport destination-port
    match interface input
    collect routing source as
    collect routing destination as
    collect routing next-hop address ipv4
    collect transport tcp flags
    collect counter bytes
    collect counter packets
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last
    collect interface output
switch#

```

Table 7 describes the significant fields shown in the display.

**Table 7** *show flow record netflow-original Field Descriptions*

Field	Description
Description	The description that you configured for the record or the default description—User defined.
No. of users	The number of references to this record in the configuration.
Total field space	The number of bytes required to store these fields for one flow.
Fields	The fields that are included in this record. For more information on the fields, refer to the <b>match</b> and <b>collect</b> commands.

#### Related Commands

Command	Description
<b>cache</b>	Configures flow cache parameters for flow monitors.
<b>clear flow monitor</b>	Clears the flow monitor.
<b>exporter</b>	Specifies a flow exporter for flow monitors.
<b>flow monitor</b>	Creates a flow monitor.
<b>protocol-distribution</b>	Configures the collection of protocol distribution statistics for flow monitors.
<b>record</b>	Configures a flow record for the flow monitor.
<b>show flow sw-monitor</b>	Displays flow monitor status and statistics.
<b>size-distribution</b>	Configures the collection of size distribution statistics for flow monitors.
<b>protocol-distribution</b>	Configures the collection of protocol distribution statistics for flow monitors.
<b>record</b>	Configures a flow record a for flow monitor.

# show flow timeout

To display the Flexible NetFlow flow cache timeout values, use the **show flow timeout** command.

## show flow timeout

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

**Defaults** Information for the Flexible NetFlow accounting configuration on the interface is displayed.

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	6.1(1)	Changed the command output.
	4.0(1)	This command was introduced.

**Usage Guidelines** You must have already enabled traffic monitoring with Flexible NetFlow before you can use the **show flow timeout** command.

This command does not require a license.

**Examples** This example shows how to display the Flexible NetFlow flow cache timeout values for F2 VDC:

```
switch# show flow timeout
Flow timeout values
  Active timeout:           1800 seconds
  Inactive timeout:        15 seconds
  Flush Cache timeout      15 seconds
  Fast timeout:             Disabled
  Session aging timeout:   Disabled
  Aggressive aging timeout: Disabled
switch#
```

Related Commands	Command	Description
	<b>flow timeout</b>	Creates a flow timeout.

# show hardware feature-capability

To display information about the registered features that are supported by the system, use the **show hardware feature-capability** command.

**show hardware feature-capability [detailed]**

Syntax Description	detailed	(Optional) Displays detailed information about registered features.
--------------------	----------	---

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

Command Modes	Any command mode
---------------	------------------

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

Release	Modification
4.2(1)	This command was introduced.

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

Examples	This example shows how to display information about the registered features that are supported by the system:
----------	---

```
switch# show hardware feature-capability detailed
Hardware Dependent Features:
. = supported
X = unsupported
-- Module --
7 12
VPC X X
module 7: Device Min num too small for feature
module 12: Device Min num too small for feature
PVLAN . .
switch#
```

Related Commands	Command	Description
	<b>show hardware capacity</b>	Displays information about the hardware capabilities and current hardware utilization by the system.

# show hardware capacity

To display information about the hardware capabilities and current hardware utilization by the system, use the **show hardware capacity** command.

**show hardware capacity [eobc | fabric-utilization | forwarding | interface | module | power]**

Syntax Description	
<b>eobc</b>	(Optional) Displays the Ethernet Out of Band Channel (EOBC) resources, such as packets per second, total packets, and dropped packets, for both ingress (rx) and egress (tx) direction.
<b>fabric-utilization</b>	(Optional) Displays switch fabric resources, such as the channel speed, the percentage of egress data, the percentage of ingress data, packet drops, peak rates, and time stamps.
<b>forwarding</b>	(Optional) Displays Layer 2 and Layer 3 forwarding resources, such as available resources, the percentage of used resources, and the percentage of free resources.
<b>interface</b>	(Optional) Displays the chassis, slot, or port number, and the ingress (rx) and egress (tx) packet drop counter against it.
<b>module</b>	(Optional) Displays information about the modules, crossbar resources, and the percentage of total, free, and used Flash and NVRAM resources in each module.
<b>power</b>	(Optional) Displays a summary of the power resources of the system.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** You can make network design plans based on the information about hardware capabilities and the current hardware utilization.

This command does not require a license.



**Examples**

This example shows how to display information about the hardware capabilities and current hardware utilization by the system:

```
switch(config)# show hardware capacity module
Supervisor Redundancy HW Mode(Dual-SUPs): Disabled
Redundancy mode: Active with no standby

Switching Resources:
-----
Module  Model Number      Part Number      Serial Number
-----
  7      N7K-M148GS-11     73-11584-02     JAF1219AGFE
  10     N7K-SUP1          73-10877-11     JAF1307ALAT
  12     NURBURGRING       73-10098-04     JAB104400P0

XBAR Resources:
-----
XbarNum Model Number      Part Number      Serial Number
-----
  1      N7K-C7018-FAB-1   73-11687-01     JAF1225AGHJ

Flash/NVRAM Resources:
-----
Usage: Module  Device      Total (KB)  Free (KB)  %Used
-----
      10      bootflash  1762048    1383980    21
      10      logflash   7997912    6840772    14
      10      slot0     2026608    1985436     2
switch(config)#
```

**Related Commands**

Command	Description
<b>show hardware fabric-utilization</b>	Displays information about fabric utilizations.
<b>show module</b>	Displays information about a module.

# show hardware capacity interface

To display information about the hardware interface resources, use the **show hardware capacity interface** command.

**show hardware capacity interface**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display information about the hardware interface resources:

```
switch(config)# show hardware capacity interface
Interface Resources

Interface drops:
  Module  Total drops                Highest drop ports
    7     Tx: 0                       -
    7     Rx: 0                       -
   12     Tx: 0                       -
   12     Rx: 0                       -

Interface buffer sizes:
  Module  Bytes: Tx buffer           Rx buffer
    7     6190631                 7743330
   12     6190631                 7743330
switch#
```

Related Commands	Command	Description
	show hardware flow utilization	Displays information about NetFlow hardware flow utilization.
	show hardware fabric-utilization	Displays information about fabric utilization.

# show hardware fabric-utilization

To display the fabric utilization values reported from a 10 millisecond measurement interval that is, the ASIC measures link utilization, use the **show hardware fabric-utilization** command.

## show hardware fabric-utilization

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the fabric utilization:

```
switch(config)# show hardware fabric-utilization
-----
Slot          Total Fabric      Utilization
              Bandwidth        Ingress % Egress %
-----
1             220 Gbps          0.00    0.00
2             92 Gbps           0.00    0.00
5             23 Gbps           0.00    0.00
6             23 Gbps           0.00    0.00
7             92 Gbps           0.00    0.00
9             46 Gbps           0.00    0.00
--More--
```

Related Commands	Command	Description
	<b>show hardware fabric-utilization</b>	Displays information about fabric utilization.

# show hardware fabric-utilization detail timestamp

To display the time and value of peak utilization timestamp, use the **show hardware fabric-utilization detail timestamp** command.

## show hardware fabric-utilization detail timestamp

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	6.1(1)	This command was introduced.

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

**Examples** This example shows how to display the time and value of peak utilization:

```
switch(config)# show hardware fabric-utilization detail timestamp
swN7K148# show hardware fabric-utilization detail timestamp
-----
Fabric Planes:
A -- Unicast fabric interface
B -- Multicast/Multidestination fabric interface
-----PEAK FABRIC UTILIZATION-----
I/O |-----FABRIC-----| Ingress | Egress
Slot |Mod Inst Plane| Util      Time      | Util      Time
-----|-----|-----|-----|-----|-----|-----|-----
2   1   1   A   0%      08-11@19:18:41  0%      08-11@19:18:41
2   1   1   B   0%      08-11@19:18:41  0%      08-11@19:18:41
2   1   1   A   0%      08-11@19:18:41  0%      08-11@19:18:41
2   1   1   B   0%      08-11@19:18:41  0%      08-11@19:18:41
2   2   1   A   0%      08-11@19:18:41  0%      08-11@19:18:41
2   2   1   B   0%      08-11@19:18:41  0%      08-11@19:18:41
2   2   1   A   0%      08-11@19:18:41  0%      08-11@19:18:41
2   2   1   B   0%      08-11@19:18:41  0%      08-11@19:18:41
2   3   1   A   0%      08-11@19:18:41  0%      08-11@19:18:41
2   3   1   B   0%      08-11@19:18:41  0%      08-11@19:18:41
2   3   1   A   0%      08-11@19:18:41  0%      08-11@19:18:41
```

### show hardware fabric-utilization detail timestamp

```

2      3      1      B      0%      08-11@19:18:41      0%      08-11@19:18:41
5      1      1      A      0%      08-11@19:18:34      0%      08-11@19:18:34
5      1      1      B      0%      08-11@19:18:34      0%      08-11@19:18:34
5      2      1      A      0%      08-11@19:18:34      0%      08-11@19:18:34
--More--

```

#### Related Commands

Command	Description
<b>show hardware fabric-utilization</b>	Displays information about fabric utilization.

# show hardware flow aging

To display information about NetFlow hardware flow aging, use the **show hardware flow aging** command.

```
show hardware flow aging [vdc vdc-name] [module slot-number]
```

Syntax Description		
<b>vdc</b> <i>vdc-name</i>	(Optional) Specifies the virtual context device (VDC) name. The VDC name can be any case-sensitive, alphanumeric string up to 64 characters.	
<b>module</b> <i>slot-number</i>	(Optional) Displays information specific to a module.	

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** You must have already enabled traffic monitoring with Flexible NetFlow before you can use the **show hardware flow aging** command.

This command does not require a license.

**Examples** This example shows how to display the NetFlow aging values for module 2:

```
switch(config)# show hardware flow aging module 2
VDC(1) Aging Information (time unit is second):

AgingType  Enabled  Timeout  Period  Threshold
-----+-----+-----+-----+-----
Active     Yes      1800     360     N/A
Inactive   Yes      15       3       N/A
Fast       Yes      33       6       22
Aggressive No       90       18      90
Session    No       2        5       N/A
switch(config)#
```

■ show hardware flow aging

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>flow timeout</b>	Creates a flow timeout.



# show hardware flow entry

To display information about a NetFlow table entry, use the **show hardware flow entry** command.

**show hardware flow entry address** *location* **type** {**ip** | **ipv6**} [**detail**] [**module** *slot-number*]

Syntax Description	Parameter	Description
	<b>address</b>	Specifies the NetFlow table address.
	<i>location</i>	Address location of the NetFlow table entry, in hexadecimal. The location range is from 0x0 to 0x3ffff.
	<b>ip</b>	Displays detailed information about the IP flows.
	<b>ipv6</b>	Displays detailed information about the IPv6 flows.
	<b>detail</b>	(Optional) Displays detailed information about the flows.
	<b>module</b> <i>slot-number</i>	(Optional) Displays information specific to a module.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** You must have already enabled traffic monitoring with Flexible NetFlow before you can use the **show hardware flow entry** command.

This command does not require a license.

**Examples** This example show how to display the NetFlow table entry for module 2:

```
switch(config)# show hardware flow entry address 0x0 type ip module 2
NT Entry Info (dev_id = 0, nt_entry_addr = 0x00000000):

protocol                = 0 (0=IPv4/IPMAC, 1=IPv6, 2=L2, 3=MPLS)
profile_id              = 0
recir_id                = 0
is_routed               = 0
from_rp                 = 0
lkup_dir                = 0 (0=Ingress, 1=Egress)
ilif(ovld_a)           = 0x0
```

## show hardware flow entry

```

elif(ovld_b)           = 0x0
tos(ovld_e)           = 0
l4_protocol           = 0
l4_hdr_vld            = 0
fragment              = 0
mpls                  = 0
l4_info(ovld_d)       = 0x00000000
ipv4_sa(ovld_f)       = 0.0.0.0
ipv4_da(ovld_g)       = 0.0.0.0
ipmac                 = 0
segment               = 0
hash_addr             = 0x0
icam                  = 0
create_ts             = 0
sh_plc_idx/sampler_id = 0x0
rdt_tbl_idx           = 0x0
ignr_aclo             = 0
ignr_qoso             = 0
ignr_acc              = 0
ignr_agg_qos          = 0
tcp_rdt_dst           = 0
copy_policy_idx       = 0x0
nf_acos               = 0
mark_en               = 0
nf_qos_mode           = 0
policer_param_idx    = 0x0
elam_trig             = 0
valid                 = 0
sw_entry              = 0
profile_merged        = 0
fast_ag_en            = 0
sw_bits1              = 0
dgt_mode              = 0
adj_ptr/dgt           = 0x0
ignr_qosi             = 0
ignr_acl_i            = 0

```

NS Entry Info (dev\_id = 0, ns\_entry\_addr = 0x00000000):

```

ack_after_fin         = 0
tcp_flag              = 0x0 (URG=0, ACK=0, PSH=0, RST=0, SYN=0, FIN=0)
mf_ls_ts              = 0
mf_bkt                = 0
nf_pkt_cnt            = 0000000000
nf_byte_cnt           = 00000000000000
nf_byte_cnt_excd      = 00000000000000
ls_used_ts            = 0
sw_prog/sticky_status = 0

```

---

**Related Commands**

Command	Description
<b>flow</b>	Creates a flow.

---

# show hardware flow

To display information about NetFlow hardware IP flows, use the **show hardware flow ip** command.

```
show hardware flow {ip | ipv6} [interface type number | monitor monitor-name | profile profile-id
| vdc vdc-name | vlan vlan-name] [detail] [module module]
```

Syntax Description		
<b>ip</b>		Displays information about the IP flows.
<b>ipv6</b>		Displays information about the IPv6 flows.
<b>interface</b> <i>interface-type number</i>	(Optional)	Specifies the type of interface that you want to view Flexible NetFlow accounting configuration information on.
<b>monitor</b> <i>monitor-name</i>	(Optional)	Specifies the name of the flow monitor. The monitor name can be any case-sensitive, alphanumeric string up to 64 characters.
<b>profile</b> <i>profile-id</i>	(Optional)	Specifies the name of the flow profile. The profile ID range is from 0 to 31.
<b>vdc</b> <i>vdc-name</i>	(Optional)	Specifies the virtual device context (VDC) name. The VDC name can be any case-sensitive, alphanumeric string up to 64 characters.
<b>detail</b>	(Optional)	Displays detailed information about the flows.
<b>module</b> <i>slot-number</i>	(Optional)	Displays information specific to a module.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** You must have already enabled traffic monitoring with Flexible NetFlow before you can use the **show hardware flow ip** command.

This command does not require a license.

**Examples** This example shows how to display the NetFlow aging values for module 8:

```
switch(config)# show hardware flow ip module 8
```

## show hardware flow

D - Direction; L4 Info - Protocol:Source Port:Destination Port  
 IF - Interface: ()ethernet, (S)vi, (V)lan, (P)ortchannel, (T)unnel  
 TCP Flags: Ack, Flush, Push, Reset, Syn, Urgent

```

D IF      SrcAddr          DstAddr          L4 Info          PktCnt          TCP Flags
-----+-----+-----+-----+-----+-----+-----
I 8/26   007.002.000.002   007.001.000.002 000:00000:00000 0000421885     . . . . .
I 8/25   007.001.000.002   007.002.000.002 000:00000:00000 0000421900     . . . . .
O 8/25   007.002.000.002   007.001.000.002 000:00000:00000 0000422213     . . . . .
O 8/26   007.001.000.002   007.002.000.002 000:00000:00000 0000422228     . . . . .
switch(config)#

```

## Related Commands

Command	Description
flow	Creates a flow.

# show hardware flow I2

To display information about NetFlow hardware Layer 2 flows, use the **show hardware flow I2** command.

```
show hardware flow I2 [monitor monitor-name | profile profile-id | vdc vdc-id | vlan vlan-id]
[detail] [instance instance] [module module]
```

## Syntax Description

<b>monitor</b> <i>monitor-name</i>	(Optional) Specifies the name of the flow monitor. The monitor name can be any case-sensitive, alphanumeric string up to 64 characters.
<b>profile</b> <i>profile-id</i>	(Optional) Specifies the name of the flow profile. The profile ID range is from 0 to 7.
<b>vdc</b>	(Optional) Specifies the virtual device context (VDC) name.
<i>vdc-id</i>	(Optional) Virtual device context ID. The range is from 1 to 16 alphanumeric string.
<b>vlan</b>	(Optional) Displays a VLAN.
<i>vlan-id</i>	(Optional) Displays VLAN ID. The range is from 1 to 4094.
<b>detail</b>	(Optional) Displays detailed information about the flows.
<b>instance</b>	(Optional) Displays information about the EARL instance.
<i>instance</i>	(Optional) Displays the instance number. The range is from 1 to 2.
<i>slot number</i>	(Optional) Specifies the slot number. The range is from 1 to 18.

## Defaults

None

## Command Modes

EXEC mode

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
5.1(1)	This command was introduced.

## Usage Guidelines

This command does not require a license.

## Examples

This example shows how to display detailed output information about the NetFlow Layer 2 flows:

```
switch(config)# show hardware flow I2 detail
D IF          SMAC          DMAC          ET  PktCnt      TCP Flags    DSCP
```



# show hardware flow sampler

To display information about sampled NetFlow hardware flows, use the **show hardware flow sampler** command.

```
show hardware flow sampler { all | count | index number | name sampler-name | vdc vdc_id }
    [detail] [module module] [instance instance]
```

Syntax Description		
<b>all</b>		Specifies all sampled NetFlow hardware flows.
<b>count</b>		Specifies the sampler table utilization.
<b>index</b> <i>number</i>		Specifies the sampler table index, in hexadecimal. The range is from 0x0 to 0x3ff.
<b>name</b> <i>sampler-name</i>		Specifies the sampler name. The name can be any case-sensitive, alphanumeric string up to 64 characters.
<b>vdc</b> <i>vdc-name</i>		Specifies the virtual device context (VDC) name. The VDC name can be any case-sensitive, alphanumeric string up to 64 characters.
<b>detail</b>		(Optional) Displays detailed information about the flows.
<b>module</b> <i>slot-number</i>		(Optional) Displays information that is specific to a module.
<b>instance</b> <i>instance</i>		(Optional) Displays the instance number.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** You must have already enabled traffic monitoring with Flexible NetFlow before you can use the **show hardware flow sampler** command.

This command does not require a license.

**Examples** This example shows how to display the NetFlow sampler table utilization for module 2:

```
switch# show hardware flow sampler count module 2
Sampler Table Utilization: about 0.00% (0/64)
```

■ show hardware flow sampler

Related Commands	Command	Description
	flow	Creates a flow.



# show hardware flow utilization

To display information about NetFlow hardware flow utilization, use the **show hardware flow utilization** command.

**show hardware flow utilization** [**module** *module*]

<b>Syntax Description</b>	<b>module</b> <i>slot-number</i> (Optional) Displays information specific to a module.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	You must have already enabled traffic monitoring with Flexible NetFlow before you can use the <b>show hardware flow utilization</b> command.  This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display the NetFlow sampler table utilization for module 2:
-----------------	---

```
switch# show hardware flow utilization module 2
Flow Utilization: 0.00% (0/515090)

Total number of flows = 0
IPv4 flow creation failure = 0
IPv6 flow creation failure = 0
MPLS flow creation failure = 0
L2 flow creation failure = 0
IFE flow creation failure = 0
OFE flow creation failure = 0
IFE CF FIFO full failure = 0
OFE CF FIFO full failure = 0
IFE NT table full failure = 0
OFE NT table full failure = 0
NO freelist pointer failure = 0
Hash Table(NH) page full failure = 0
IPMAC lookup failure = 0
L2 ACL deny = 0
```

## ■ show hardware flow utilization

```
L3 ACL deny           = 0
IFE CF flow control   = 0
OFE CF flow control   = 0
Fast Aging failure    = 0
switch#
```

---

**Related Commands**

---

<b>Command</b>	<b>Description</b>
<b>flow</b>	Creates a flow.

---



## ■ show hardware internal rxwait-history

```
RxWait per second (last 60 seconds)
# = RxWait (ms)
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show hardware internal</b>	Displays information of the physical device hardware.

---



## ■ show hardware internal txwait-history

```
Pause TxWait per second (last 60 seconds)
# = TxWait (ms)
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show hardware internal</b>	Displays information of the physical device hardware.

---

# show icam entries acl

To display the traffic analytics of the access control list (ACL) ternary content addressable memory (TCAM), which includes RACL, VACL, QoS, PBR, WCCP, CoPP, and so on, use the **show icam entries acl** command.

```
show icam entries acl module module inst instance [history num-intervals][sort {[filter
feature-name [exact]}][sort-order sort-order-list][top top-percentage}}
```

Syntax Description		
<b>acl</b>		Specifies TCAM entries.
<b>module</b> <i>module</i>		Specifies the module number. The range is from 1–18 for an 18-slot chassis, and from 1–9 for a 9-slot chassis.
<b>inst</b> <i>instance</i>		Specifies the ASIC or forwarding engine instance number. The range is from 0–11.
<b>history</b>		(Optional) Displays the history of entries.
<i>num-intervals</i>		Number of intervals in the history. The range is from 168–1344.
<b>sort</b>		(Optional) Specifies the sorted display.
<b>sort-order</b> <i>sort-order-list</i>		(Optional) Displays the sorted entries in a specific order; <b>1</b> for ascending order and <b>2</b> for descending order. The entries are sorted in descending order by default.
<b>filter</b> <i>feature-name</i>		(Optional) Specifies the feature name to be filtered. By default, all the features are displayed. Enclose the feature name in quotation marks if it contains more than one word, for example, QoS COPP.
<b>exact</b>		(Optional) Filters the TCAM entries based on the exact feature name, which has one word. This keyword can be used only when filtering the TCAM entries by feature names.
<b>top</b> <i>top-percentage</i>		(Optional) Displays the top TCAM entries based on the specified percentage. The range is from 1–100. The default is 1.

**Command Default** The top 1 percent TCAM entries are displayed in descending order.

**Command Modes** Any command mode

Command History	Release	Modification
	Cisco NX-OS Release 8.2(1)	This command was modified. The following keywords and arguments were added: <ul style="list-style-type: none"> <li><b>history</b> <i>num-intervals</i></li> <li><b>exact</b></li> </ul>
	Cisco NX-OS Release 8.0(1)	This command was introduced.

**Usage Guidelines**

- To view the history of TCAM entries utilization, enable iCAM monitoring on the required entries using the **icam monitor entries** command.
- To filter the TCAM entries using the **sort** keyword, use at least one option following this keyword.

**Examples**

This example shows how to view iCAM monitoring of the TCAM entries for a current date:

```
switch# show icam entries acl module 3 inst 5
Retrieving data from linecard. This may take some time ...
=====
TCAM Entries (Mod 3,Inst 5)
-----
Feature  Pkt_Type                               Source IP/Mask Dest IP/Mask   Action
ifindex   Stats
-----
          FEX    IPv4                               ip 0.0.0.0/0 0.0.0.0/0
Redirect  0x15090000                                0
          FEX    IPv6  ip 0x00000000000000000000000000000000/0 0x00000000000000000000000000000000
Redirect  0x15090000                                0
          FEX    MAC    0000.0000.0000 0000.0000.0000 0000.0000.0000 0000.0000.0000
Redirect  0x15090000                                0
          FEX    ARP  arp-rarp/all ip 0.0.0.0/0 0.0.0.0/0 0000.0000.0000 0000.0000.00
Redirect  0x15090000                                0
          RACL   IPv4                               tcp 209.165.200.225/27 0.0.0.0/0
Permit   0x1a10a000                                0
          RACL   IPv4                               tcp 209.165.201.1/27 0.0.0.0/0
Permit   0x1a10a000                                0
          RACL   IPv4                               tcp 209.165.202.129/27 0.0.0.0/0
Permit   0x1a10a000                                0
          RACL   IPv4                               tcp 209.165.202.139/27 0.0.0.0/0
Permit   0x1a10a000                                0
          RACL   IPv4                               tcp 209.165.202.140/27 0.0.0.0/0
Permit   0x1a10a000                                0
          QoS  COPP   IPv4                               udp 0.0.0.0/0 209.165.201.3/27
QoS      0x0                                0
          QoS  COPP   IPv4                               udp 0.0.0.0/0 209.165.201.3/27
QoS      0x0                                0
          QoS  COPP   IPv4                               209.165.201.1/27 0.0.0.0/0
QoS      0x0                                0
          QoS  COPP   IPv4                               udp 0.0.0.0/0 209.165.201.1/27
QoS      0x0                                0
          QoS  COPP   IPv4                               udp 0.0.0.0/0 209.165.201.1/27
QoS      0x0                                0
          QoS  COPP   IPv4                               udp 0.0.0.0/0 209.165.201.7/27
QoS      0x0                                0
          QoS  COPP   IPv4                               udp 0.0.0.0/0 209.165.201.7/27
QoS      0x0                                0
          QoS  COPP   IPv4                               udp 0.0.0.0/0 209.165.201.11/27
QoS      0x0                                0
          QoS  COPP   IPv4                               udp 0.0.0.0/0 209.165.201.11/27
QoS      0x0                                0
          QoS  COPP   IPv4                               ip 0.0.0.0/0 209.165.201.14/27
QoS      0x0                                0
```

This example shows how to view the top TCAM entries that are monitored by iCAM for a current date filtered by a feature name:

```
switch# show icam entries acl module 3 inst 5 sort filter "qos copp" top 10
Retrieving data from linecard. This may take some time ...
=====
TCAM Entries (Mod 3,Inst 5)
```



```

-----
-----
Feature Pkt_Type Source IP/Mask Dest IP/Mask
Action  ifindex      Stats
-----
-----
QoS COPP  IPv4                               ip 0.0.0.0/0 0.0.0.0/0
QoS      0x0          38408890
QoS COPP  MAC 0000.0000.0000 0000.0000.0000 0180.c200.000e ffff.ffff.ffff 350
QoS      0x0          254
QoS COPP  MAC 0000.0000.0000 0000.0000.0000 0100.0ccc.cccc ffff.ffff.ffff
QoS      0x0          23
QoS COPP  IPv4                               udp 0.0.0.0/0 209.165.201.1/27
QoS      0x0          0
QoS COPP  IPv4                               udp 0.0.0.0/0 209.165.201.1/27
QoS      0x0          0
-----

```

This example shows how to view iCAM monitoring of the TCAM entries for a current date filtered by a feature name using the **exact** keyword:

```

switch# show icam entries acl module 7 inst 0 sort filter QoS exact top 100
Retrieving data from linecard. This may take some time ...
=====
TCAM Entries (Mod 7,Inst 0)
-----
-----
Feature Pkt_Type Source IP/Mask Dest IP/Mask Action
Action  ifindex  Stats
-----
-----
QoS IPv4 ip 209.165.201.1/27 209.165.202.129/27 QoS
0x1a316000 0
QoS IPv4 ip 209.165.201.1/27 209.165.202.129/27 QoS
0x1a316000 0
QoS IPv4 ip 209.165.201.2/27 209.165.202.129/27 QoS
0x1a316000 0
QoS IPv4 ip 209.165.201.2/27 209.165.202.129/27 QoS
0x1a316000 0
QoS IPv4 ip 209.165.201.3/27 209.165.202.129/27 QoS
0x1a316000 0
QoS IPv4 ip 209.165.201.3/27 209.165.202.129/27 QoS
0x1a316000 0
QoS IPv4 ip 0.0.0.0/0 0.0.0.0/0 QoS
0x1a316000 0
QoS IPv4 ip 0.0.0.0/0 0.0.0.0/0 QoS
0x1a316000 0
-----

```

This example shows how to view the history of TCAM entries monitored by iCAM:

```

switch# show icam entries acl module 3 inst 5 history 2
=====
TCAM Entries (Mod 3,Inst 5): Cumulative stats for last 2 intervals
-----
-----
Feature Pkt_Type Source IP/Mask Dest IP/Mask
Action  ifindex  Stats Rate(pps)
-----
-----
-----

```

## show icam entries acl

```

      FEX    IPv4
Redirect 0x15090000          0          0          ip 0.0.0.0/0 0.0.0.0/0
      FEX    IPv6  ip 0x00000000000000000000000000000000/0 0x000000000000000000000000
Redirect 0x15090000          0          0
      FEX    MAC    0000.0000.0000 0000.0000.0000 0000.0000.0000 0000.0000.0000
Redirect 0x15090000          0          0
      FEX    ARP    arp-rarp/all ip 0.0.0.0/0 0.0.0.0/0 0000.0000.0000 0000.0000.00
Redirect 0x15090000          0          0
      RACL   IPv4
Permit  0x1a10a000          0          0          tcp 209.165.201.1/27 0.0.0.0/0
      RACL   IPv4
Permit  0x1a10a000          0          0          tcp 209.165.201.2/27 0.0.0.0/0
      RACL   IPv4
Permit  0x1a10a000          0          0          tcp 209.165.201.3/27 0.0.0.0/0
      RACL   IPv4
Permit  0x1a10a000          0          0          tcp 209.165.201.4/27 0.0.0.0/0
      RACL   IPv4
Permit  0x1a10a000          0          0          tcp 209.165.201.5/27 0.0.0.0/0
      RACL   IPv4
Permit  0x1a10a000          0          0
      QoS   COPP   IPv4
QoS     0x0          0          0          udp 0.0.0.0/0 209.165.201.1/27
      QoS   COPP   IPv4
QoS     0x0          0          0          udp 0.0.0.0/0 209.165.201.1/27
      QoS   COPP   IPv4
QoS     0x0          0          0          udp 0.0.0.0/0 209.165.201.1/27
      QoS   COPP   IPv4
QoS     0x0          0          0          udp 0.0.0.0/0 209.165.201.1/27
      QoS   COPP   IPv4
QoS     0x0          0          0          udp 0.0.0.0/0 209.165.201.1/27
      QoS   COPP   IPv4
QoS     0x0          0          0          udp 0.0.0.0/0 209.165.201.7/27
      QoS   COPP   IPv4
QoS     0x0          0          0          udp 0.0.0.0/0 209.165.201.7/27
      QoS   COPP   IPv4
QoS     0x0          0          0          udp 0.0.0.0/0 209.165.201.11/27
      QoS   COPP   IPv4
QoS     0x0          0          0          udp 0.0.0.0/0 209.165.201.11/27
      QoS   COPP   IPv4
QoS     0x0          0          0

```

This example shows how to view the history of the top 1 percent TCAM entries filtered by a feature name:

```

switch# show icam entries acl module 3 inst 5 history 2 sort filter "qos copp" top 1
=====
TCAM Entries (Mod 3,Inst 5): Cumulative stats for last 2 intervals
-----

```

Action	Feature	Pkt_Type	ifindex	Stats	Rate(pps)	Source IP/Mask	Dest IP/Mask
QoS	COPP	MAC	0x0	0000.0000.0000 48	0000.0000.0000 0	0180.c200.000e ffff.ffff.ffff	350
QoS	COPP	MAC	0x0	0000.0000.0000 4	0000.0000.0000 0	0100.0ccc.cccc ffff.ffff.ffff	
QoS	COPP	IPv4	0x0	0	0	tcp 0.0.0.0/0	0.0.0.0/0
QoS	COPP	IPv4	0x0	0	0	tcp 0.0.0.0/0	0.0.0.0/0

This example shows how to view the history of the top 2 percent TCAM entries filtered by a feature name:

```

switch# show icam entries acl module 3 inst 5 history 2 sort filter "qos copp" top 2

```

```

=====
TCAM Entries (Mod 3,Inst 5): Cumulative stats for last 2 intervals
-----

```

Feature	Pkt_Type	Stats	Rate(pps)	Source IP/Mask	Dest IP/Mask
Action	ifindex				
QoS COPP	MAC	0000.0000.0000	0000.0000.0000	0180.c200.000e	ffff.ffff.ffff 350
QoS	0x0	48	0		
QoS COPP	MAC	0000.0000.0000	0000.0000.0000	0100.0ccc.cccc	ffff.ffff.ffff
QoS	0x0	4	0		
QoS COPP	IPv4			tcp 0.0.0.0/0	0.0.0.0/0
QoS	0x0	0	0		
QoS COPP	IPv4			tcp 0.0.0.0/0	0.0.0.0/0
QoS	0x0	0	0		
QoS COPP	IPv4			tcp 0.0.0.0/0	0.0.0.0/0
QoS	0x0	0	0		
QoS COPP	IPv4			tcp 0.0.0.0/0	0.0.0.0/0
QoS	0x0	0	0		
QoS COPP	IPv4			udp 0.0.0.0/0	209.165.201.1/27
QoS	0x0	0	0		

This example shows how to view iCAM monitoring of the TCAM entries for a current date filtered by a feature name:

```

switch# show icam entries acl module 3 inst 5 sort filter "qos copp"
Retrieving data from linecard. This may take some time ...
=====
TCAM Entries (Mod 3,Inst 5)
-----

```

Feature	Pkt_Type	Stats	Source IP/Mask	Dest IP/Mask
Action	ifindex			
QoS COPP	IPv4		ip 0.0.0.0/0	0.0.0.0/0
QoS	0x0	38408890		
QoS COPP	MAC	0000.0000.0000	0000.0000.0000	0180.c200.000e 350
QoS	0x0	249		
QoS COPP	MAC	0000.0000.0000	0000.0000.0000	0100.0ccc.cccc 350
QoS	0x0	22		
QoS COPP	IPv4		tcp 0.0.0.0/0	0.0.0.0/0
QoS	0x0	0		

### Related Commands

Command	Description
<b>feature icam</b>	Enables the iCAM feature.
<b>icam monitor entries</b>	Enables iCAM monitoring on TCAM entries.
<b>icam monitor interval</b>	Configures the iCAM monitor interval and the number of intervals in an iCAM monitor history.
<b>icam monitor resource</b>	Enables iCAM monitoring on TCAM resources.
<b>show icam entries multicast</b>	Displays traffic analytics of multicast entries.
<b>show icam prediction entries acl</b>	Displays machine-learning predictive analytics of TCAM entries.

<b>Command</b>	<b>Description</b>
<b>show icam prediction entries multicast</b>	Displays machine-learning predictive analytics of multicast entries.
<b>show icam prediction resource</b>	Displays machine-learning predictive analytics of TCAM resource utilization.
<b>show icam resource</b>	Displays TCAM resource utilization.

# show icam entries multicast

To display the traffic analytics of multicast entries, use the **show icam entries multicast** command.

```
show icam entries multicast module module [history num-intervals][sort {sort-order
sort-order-list | top top-percentage}]
```

## Syntax Description

<b>multicast</b>	Specifies multicast entries.
<b>module</b> <i>module</i>	Specifies the module number. The range is from 1–18 for an 18-slot chassis, and from 1–9 for a 9-slot chassis.
<b>inst</b> <i>instance</i>	Specifies the ASIC or forwarding engine instance number. The range is from 0–11.
<b>history</b>	(Optional) Displays the history of entries.
<i>num-intervals</i>	Number of intervals in history. The range is from 168–1344.
<b>sort</b>	(Optional) Specifies the sorted display.
<b>sort-order</b> <i>sort-order-list</i>	(Optional) Displays the sorted entries in specific order. <b>1</b> sorts the entries in ascending order and <b>2</b> sorts the entries in descending order. The entries are sorted in descending order by default.
<b>top</b> <i>top-percentage</i>	(Optional) Displays the top multicast entries based on the specified percentage. The range is from 1–100. The default is 1.

## Command Default

The top 1 percent multicast entries are displayed in descending order.

## Command Modes

Any command mode

## Command History

Release	Modification
Cisco NX-OS Release 8.2(1)	This command was modified. The following keywords and arguments were added: <ul style="list-style-type: none"> <li><b>multicast</b></li> <li><b>history</b> <i>num-intervals</i></li> </ul>
Cisco NX-OS Release 8.0(1)	This command was introduced.

## Usage Guidelines

To view the history of the utilization of multicast entries, you must enable Intelligent CAM (iCAM) monitoring on the required entries using the **icam monitor entries** command.

## Examples

This example shows how to view iCAM monitoring of multicast entries for a current date:

```
switch# show icam entries multicast module 3
Retrieving data from linecard. This may take some time ...
```

## show icam entries multicast

```

=====
Multicast Entries (Mod 3)
-----
-----
VDC_ID      TABLE_ID  Source/Mask  Group/Mask  RPF
Stats
-----
-----
1           1           0.0.0.0/0    209.165.201.9/27
1
1           1           209.165.201.18/27  209.165.201.10/27  Ethernet3/12
912494
1           1           209.165.201.19/27  209.165.201.10/27  Ethernet3/12
912494
1           1           209.165.201.20/27  209.165.201.10/27  Ethernet3/12
912494
1           1           209.165.201.21/27  209.165.201.10/27  Ethernet3/12
912493
1           1           209.165.201.22/27  209.165.201.10/27  Ethernet3/12
912493
1           1           209.165.201.23/27  209.165.201.10/27  Ethernet3/12
912493
1           1           209.165.201.24/27  209.165.201.10/27  Ethernet3/12
912493
1           1           209.165.201.25/27  209.165.201.10/27  Ethernet3/12
912493
1           1           209.165.201.26/27  209.165.201.10/27  Ethernet3/12
912480
1           1           209.165.201.27/27  209.165.201.10/27  Ethernet3/12
912479
1           1           209.165.201.28/27  209.165.201.10/27  Ethernet3/12
912479
1           1           209.165.201.29/27  209.165.201.10/27  Ethernet3/12
912479
1           1           209.165.201.30/27  209.165.201.10/27  Ethernet3/12
912479
1           1           209.165.202.129/27  209.165.201.10/27  Ethernet3/12
912479
1           1           209.165.202.130/27  209.165.201.10/27  Ethernet3/12
912479
1           1           209.165.202.131/27  209.165.201.10/27  Ethernet3/12
912471
1           1           209.165.202.132/27  209.165.201.10/27  Ethernet3/12
912470
1           1           209.165.202.133/27  209.165.201.10/27  Ethernet3/12
912470
1           1           209.165.202.134/27  209.165.201.10/27  Ethernet3/12
912442
1           1           209.165.202.135/27  209.165.201.10/27  Ethernet3/12
912442
1           1           209.165.202.136/27  209.165.201.10/27  Ethernet3/12
912442
1           1           209.165.202.137/27  209.165.201.10/27  Ethernet3/12
912441
1           1           209.165.202.138/27  209.165.201.10/27  Ethernet3/12
912441
1           1           209.165.202.139/27  209.165.201.10/27  Ethernet3/12
912441
1           1           209.165.202.140/27  209.165.201.10/27  Ethernet3/12
912441
1           1           209.165.202.141/27  209.165.201.10/27  Ethernet3/12
912431

```

```

          1          1  209.165.202.142/27      209.165.201.10/27  Ethernet3/12
912431
          1          1  209.165.202.143/27      209.165.201.10/27  Ethernet3/12
912431
          1          1  209.165.202.144/27      209.165.201.10/27  Ethernet3/12
912431
          1          1  209.165.202.145/27      209.165.201.10/27  Ethernet3/12
912411
          1          1  209.165.202.146/27      209.165.201.10/27  Ethernet3/12
912412
          1          1  209.165.202.147/27      209.165.201.10/27  Ethernet3/12
912411
          1          1  209.165.202.148/27      209.165.201.10/27  Ethernet3/12
912411
          1          1  209.165.202.149/27      209.165.201.10/27  Ethernet3/12
912411
          1          1  209.165.202.150/27      209.165.201.10/27  Ethernet3/12
912345
          1          1  209.165.202.151/27      209.165.201.10/27  Ethernet3/12
912345
          1          1  209.165.202.152/27      209.165.201.10/27  Ethernet3/12
912345
          1          1  209.165.202.153/27      209.165.201.10/27  Ethernet3/12
912345
          1          1  209.165.202.154/27      209.165.201.10/27  Ethernet3/12
912345
          1          1  209.165.202.155/27      209.165.201.10/27  Ethernet3/12
912345
          1          1  209.165.202.156/27      209.165.201.10/27  Ethernet3/12
912344
          1          1  209.165.202.157/27      209.165.201.10/27  Ethernet3/12
912333
          1          1  209.165.202.158/27      209.165.201.10/27  Ethernet3/12
912333
    
```

This example shows how to view the top multicast entries monitored by iCAM for a current date:

```

switch# show icam entries multicast module 3 sort top 1
Retrieving data from linecard. This may take some time ...
=====
Multicast Entries (Mod 3)
-----
-----
      VDC_ID      TABLE_ID      Source/Mask      Group/Mask      RPF
Stats
-----
          1          1  209.165.200.225/27      209.165.201.10/27  Ethernet3/12
933495
          1          1  209.165.200.226/27      209.165.201.10/27  Ethernet3/12
933491
          1          1  209.165.200.227/27      209.165.201.10/27  Ethernet3/12
933488
          1          1  209.165.200.228/27      209.165.201.10/27  Ethernet3/12
933483
          1          1  209.165.200.229/27      209.165.201.10/27  Ethernet3/12
933483
          1          1  209.165.200.230/27      209.165.201.10/27  Ethernet3/12
933480
          1          1  209.165.200.231/27      209.165.201.10/27  Ethernet3/12
933476
    
```

## show icam entries multicast

```

1          1  209.165.200.232/27    209.165.201.10/27  Ethernet3/12
933474
1          1  209.165.200.233/27    209.165.201.10/27  Ethernet3/12
933469
1          1  209.165.200.234/27    209.165.201.10/27  Ethernet3/12
933469
1          1  209.165.200.235/27    209.165.201.10/27  Ethernet3/12
933466
1          1  209.165.200.236/27    209.165.201.10/27  Ethernet3/12
933462
1          1  209.165.200.237/27    209.165.201.10/27  Ethernet3/12
933456
1          1  209.165.200.238/27    209.165.201.10/27  Ethernet3/12
933455
1          1  209.165.201.1/27      209.165.201.10/27  Ethernet3/12
933455
1          1  209.165.201.2/27     209.165.201.10/27  Ethernet3/12
933452
1          1  209.165.201.3/27     209.165.201.10/27  Ethernet3/12
933449
1          1  209.165.201.4/27     209.165.201.10/27  Ethernet3/12
933442
1          1  209.165.201.5/27     209.165.201.10/27  Ethernet3/12
933441
1          1  209.165.201.6/27     209.165.201.10/27  Ethernet3/12
933441
1          1  209.165.201.7/27     209.165.201.10/27  Ethernet3/12
933441
1          1  209.165.201.8/27     209.165.201.10/27  Ethernet3/12
933435
1          1  209.165.201.9/27     209.165.201.10/27  Ethernet3/12
933434
1          1  209.165.201.11/27    209.165.201.10/27  Ethernet3/12
933418
1          1  209.165.201.12/27    209.165.201.10/27  Ethernet3/12
933202
1          1  209.165.201.13/27    209.165.201.10/27  Ethernet3/12
933202
1          1  209.165.201.14/27    209.165.201.10/27  Ethernet3/12
933202
1          1  209.165.201.15/27    209.165.201.10/27  Ethernet3/12
933202
1          1  209.165.201.16/27    209.165.201.10/27  Ethernet3/12
933202
1          1  209.165.201.17/27    209.165.201.10/27  Ethernet3/12
933202
1          1  209.165.201.18/27    209.165.201.10/27  Ethernet3/12
933202
1          1  209.165.201.19/27    209.165.201.10/27  Ethernet3/12
933202
1          1  209.165.201.20/27    209.165.201.10/27  Ethernet3/12
933188
1          1  209.165.201.21/27    209.165.201.10/27  Ethernet3/12
933187
1          1  209.165.201.22/27    209.165.201.10/27  Ethernet3/12
933187
1          1  209.165.201.23/27    209.165.201.10/27  Ethernet3/12
933187
1          1  209.165.201.24/27    209.165.201.10/27  Ethernet3/12
933187
1          1  209.165.201.25/27    209.165.201.10/27  Ethernet3/12
933187
1          1  209.165.201.26/27    209.165.201.10/27  Ethernet3/12
933187

```



```

          1          1  209.165.201.27/27      209.165.201.10/27  Ethernet3/12
933179
          1          1  209.165.201.28/27      209.165.201.10/27  Ethernet3/12
933178
          1          1  209.165.201.29/27      209.165.201.10/27  Ethernet3/12
933178
          1          1  209.165.201.30/27      209.165.201.10/27  Ethernet3/12
933150
          1          1  209.165.202.129/27     209.165.201.10/27  Ethernet3/12
933150
          1          1  209.165.202.130/27     209.165.201.10/27  Ethernet3/12
933150
          1          1  209.165.202.131/27     209.165.201.10/27  Ethernet3/12
933149
          1          1  209.165.202.132/27     209.165.201.10/27  Ethernet3/12
933149
          1          1  209.165.202.133/27     209.165.201.10/27  Ethernet3/12
933149
          1          1  209.165.202.134/27     209.165.201.10/27  Ethernet3/12
933149
          1          1  209.165.202.135/27     209.165.201.10/27  Ethernet3/12
933139
    
```

This example shows how to view the history of multicast entries monitored by iCAM:

```

switch# show icam entries multicast module 3 history 2
=====
Multicast Entries (Mod 3): Cumulative stats for last 2 intervals
-----
-----
      VDC_ID      TABLE_ID      Source/Mask      Group/Mask      RPF
Stats      Rate(pps)
-----
          1          1          0.0.0.0/0      209.165.201.9/27
0
          1          1      209.165.201.18/27      209.165.201.10/27  Ethernet3/12
165792          690
          1          1      209.165.201.19/27      209.165.201.10/27  Ethernet3/12
165792          690
          1          1      209.165.201.20/27      209.165.201.10/27  Ethernet3/12
165793          690
          1          1      209.165.201.21/27      209.165.201.10/27  Ethernet3/12
165793          690
          1          1      209.165.201.22/27      209.165.201.10/27  Ethernet3/12
165792          690
          1          1      209.165.201.23/27      209.165.201.10/27  Ethernet3/12
165792          690
          1          1      209.165.201.24/27      209.165.201.10/27  Ethernet3/12
165792          690
          1          1      209.165.201.25/27      209.165.201.10/27  Ethernet3/12
165792          690
          1          1      209.165.201.26/27      209.165.201.10/27  Ethernet3/12
165792          690
          1          1      209.165.201.27/27      209.165.201.10/27  Ethernet3/12
165792          690
          1          1      209.165.201.28/27      209.165.201.10/27  Ethernet3/12
165792          690
          1          1      209.165.201.29/27      209.165.201.10/27  Ethernet3/12
165792          690
    
```

## show icam entries multicast

```

1          1 209.165.201.30/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.129/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.130/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.131/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.132/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.133/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.134/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.135/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.136/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.137/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.138/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.139/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.140/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.141/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.142/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.143/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.144/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.145/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.146/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.147/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.148/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.149/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.150/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.151/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.152/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.153/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.154/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.155/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.156/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.157/27 209.165.201.10/27 Ethernet3/12
165792    690
1          1 209.165.202.158/27 209.165.201.10/27 Ethernet3/12
165792    690
.
.

```

This example shows how to view the history of top 1 percent multicast entries monitored by iCAM:

```
switch# show icam entries multicast module 3 history 2 sort top 1
=====
Multicast Entries (Mod 3): Cumulative stats for last 2 intervals
-----
-----
VDC_ID      TABLE_ID      Source/Mask      Group/Mask      RPF
Stats      Rate(pps)
-----
-----
1          1      209.165.200.225/27      209.165.201.10/27      Ethernet3/12
165725      690
1          1      209.165.200.226/27      209.165.201.10/27      Ethernet3/12
165725      690
1          1      209.165.200.227/27      209.165.201.10/27      Ethernet3/12
165725      690
1          1      209.165.200.228/27      209.165.201.10/27      Ethernet3/12
165725      690
1          1      209.165.200.229/27      209.165.201.10/27      Ethernet3/12
165725      690
1          1      209.165.200.230/27      209.165.201.10/27      Ethernet3/12
165725      690
1          1      209.165.200.231/27      209.165.201.10/27      Ethernet3/12
165725      690
1          1      209.165.200.232/27      209.165.201.10/27      Ethernet3/12
165725      690
1          1      209.165.200.233/27      209.165.201.10/27      Ethernet3/12
165725      690
1          1      209.165.200.234/27      209.165.201.10/27      Ethernet3/12
165725      690
1          1      209.165.200.235/27      209.165.201.10/27      Ethernet3/12
165724      690
1          1      209.165.200.236/27      209.165.201.10/27      Ethernet3/12
165724      690
1          1      209.165.200.237/27      209.165.201.10/27      Ethernet3/12
165724      690
1          1      209.165.200.238/27      209.165.201.10/27      Ethernet3/12
165724      690
1          1      209.165.201.1/27        209.165.201.10/27      Ethernet3/12
165724      690
1          1      209.165.201.2/27        209.165.201.10/27      Ethernet3/12
165724      690
1          1      209.165.201.3/27        209.165.201.10/27      Ethernet3/12
165724      690
1          1      209.165.201.4/27        209.165.201.10/27      Ethernet3/12
165724      690
1          1      209.165.201.5/27        209.165.201.10/27      Ethernet3/12
165724      690
1          1      209.165.201.6/27        209.165.201.10/27      Ethernet3/12
165724      690
1          1      209.165.201.7/27        209.165.201.10/27      Ethernet3/12
165724      690
1          1      209.165.201.8/27        209.165.201.10/27      Ethernet3/12
165724      690
1          1      209.165.201.9/27        209.165.201.10/27      Ethernet3/12
165724      690
1          1      209.165.201.11/27       209.165.201.10/27      Ethernet3/12
165724      690
```

## show icam entries multicast

```

1          1  209.165.201.12/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.13/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.14/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.15/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.16/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.17/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.18/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.19/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.20/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.21/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.22/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.23/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.24/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.25/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.26/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.27/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.28/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.29/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.201.30/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.202.129/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.202.130/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.202.131/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.202.132/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.202.133/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.202.134/27  209.165.201.10/27  Ethernet3/12
165724    690
1          1  209.165.202.135/27  209.165.201.10/27  Ethernet3/12
165724    690

```

## Related Commands

Command	Description
<b>feature icam</b>	Enables the iCAM feature.
<b>icam monitor entries</b>	Enables iCAM monitoring on TCAM entries.
<b>icam monitor interval</b>	Configures the iCAM monitor interval and the number of intervals in an iCAM monitor history.
<b>icam monitor resource</b>	Enables iCAM monitoring on TCAM resources.

<b>Command</b>	<b>Description</b>
<b>show icam entries acl</b>	Displays traffic analytics of the ACL TCAM, which includes RACL, VACL, QoS, PBR, WCCP, CoPP, and so on.
<b>show icam prediction entries acl</b>	Displays machine-learning predictive analytics of TCAM entries.
<b>show icam prediction entries multicast</b>	Displays machine-learning predictive analytics of multicast entries.
<b>show icam prediction resource</b>	Displays machine-learning predictive analytics of TCAM resource utilization.
<b>show icam resource</b>	Displays the TCAM resource utilization.

# show icam prediction entries acl

To display machine-learning predictive analytics of TCAM entries, use the **show icam prediction entries acl** command.

```
show icam prediction entries acl module module inst instance year month day time [top
top-percentage]
```

Syntax Description	Parameter	Description
	<b>acl</b>	Specifies TCAM entries.
	<b>module</b> <i>module</i>	Specifies the module number. The range is from 1–18 for an 18-slot chassis, and from 1–9 for a 9-slot chassis.
	<b>inst</b> <i>instance</i>	Specifies the ASIC or forwarding engine instance number. The range is from 0–11.
	<i>year</i>	Year in YYYY format. The values range from 1970–2030.
	<i>month</i>	Month in MMM format, for example, Jan, Feb, and so on. The values are case sensitive.
	<i>day</i>	Day of the month in DD format. The range is from 1–31.
	<i>time</i>	Time in HH:MM:SS format.
	<b>top</b> <i>top-percentage</i>	(Optional) Displays the predictive analytics of top TCAM entries based on the specified percentage. The range is from 1–10. The default is 1.

**Command Default** The predictive analytics of the top 1 percent TCAM entries are displayed.

**Command Modes** Any command mode

Command History	Release	Modification
	Cisco NX-OS Release 8.2(1)	This command was introduced.

**Usage Guidelines** To view predictive analytics of TCAM entries, you must enable Intelligent CAM (iCAM) monitoring on the corresponding entries using the **icam monitor entries** command.

**Examples** This example shows how to view the predictive analytics of TCAM entries:

```
switch# show icam prediction entries acl module 3 inst 5 2018 Jan 27 11:35:30
Generating predictions, this may take some time ...
```

```
=====
TCAM Entries Prediction (Mod 3,Inst 5)
```

```
-----
Feature  Pkt_Type                               Source IP/Mask Dest IP/Mask
Action   ifindex                                     Stats           Prediction
```

```

-----
QoS COPP IPv4 ip 0.0.0.0/0 0.0.0.0/0
QoS 0x0 38408890 38408890
QoS COPP MAC 0000.0000.0000 0000.0000.0000 0180.c200.000e ffff.ffff.ffff 350
QoS 0x0 485 501
QoS COPP MAC 0000.0000.0000 0000.0000.0000 0100.0ccc.cccc ffff.ffff.ffff
QoS 0x0 42 43
FEX IPv4 ip 0.0.0.0/0 0.0.0.0/0
Redirect 0x15090000 0 0
    
```

This example shows how to display the predictive analytics of the top 2 percent TCAM entries:

```

switch# show icam prediction entries acl module 3 inst 5 2018 Jan 27 11:35:30 top 2
Generating predictions, this may take some time ...
    
```

```

=====
TCAM Entries Prediction (Mod 3,Inst 5)
-----
    
```

Feature	Pkt_Type	Stats	Prediction
Action	ifindex		Source IP/Mask Dest IP/Mask
QoS COPP	IPv4		ip 0.0.0.0/0 0.0.0.0/0
QoS	0x0	38408890 38408890	
QoS COPP	MAC	0000.0000.0000 0000.0000.0000	0180.c200.000e ffff.ffff.ffff 350
QoS	0x0	485 501	
QoS COPP	MAC	0000.0000.0000 0000.0000.0000	0100.0ccc.cccc ffff.ffff.ffff
QoS	0x0	42 43	
FEX	IPv6	ip 0x00000000000000000000000000000000/0	0x00000000000000000000
Redirect	0x15090000	0	0
FEX	IPv4		ip 0.0.0.0/0 0.0.0.0/0
Redirect	0x15090000	0	0
FEX	ARP	arp-rarp/all ip 0.0.0.0/0 0.0.0.0/0	0000.0000.0000 0000.0000.00
Redirect	0x15090000	0	0
FEX	MAC	0000.0000.0000 0000.0000.0000	0000.0000.0000 0000.0000.0000
Redirect	0x15090000	0	0

**Related Commands**

Command	Description
<b>feature icam</b>	Enables the iCAM feature.
<b>icam monitor entries</b>	Enables iCAM monitoring on TCAM entries.
<b>icam monitor interval</b>	Configures the iCAM monitor interval and the number of intervals in an iCAM monitor history.
<b>icam monitor resource</b>	Enables iCAM monitoring on TCAM resources.
<b>show icam entries acl</b>	Displays traffic analytics of the ACL TCAM, which includes RAACL, VAACL, QoS, PBR, WCCP, CoPP, and so on.
<b>show icam entries multicast</b>	Displays traffic analytics of multicast entries.
<b>show icam prediction entries multicast</b>	Displays machine-learning predictive analytics of multicast entries.

<b>Command</b>	<b>Description</b>
<b>show icam prediction resource</b>	Displays machine-learning predictive analytics of TCAM resource utilization.
<b>show icam resource</b>	Displays TCAM resource utilization.



# show icam prediction entries multicast

To display machine-learning predictive analytics of multicast entries with results and statistics, use the **show icam prediction entries** command.

**show icam prediction entries multicast module** *module year month day time* [**top** *top-percentage*]

## Syntax Description

<b>multicast</b>	Specifies multicast entries.
<b>module</b> <i>module</i>	Specifies the module number. The range is from 1 to 18 for an 18-slot chassis, and the range is from 1 to 9 for a 9-slot chassis.
<b>inst</b> <i>instance</i>	Specifies the ASIC or forwarding engine instance number. The range is from 0 to 11.
<i>year</i>	Year in YYYY format. The values range from 1970 to 2030.
<i>month</i>	Month in MMM format, for example, Jan, Feb, and so on. The values are case sensitive.
<i>day</i>	Day of the month in DD format. The range is from 1 to 31.
<i>time</i>	Time in HH:MM:SS format.
<b>top</b> <i>top-percentage</i>	(Optional) Displays predictive analytics of top multicast entries based on the specified percentage. The range is from 1 to 10. The default is 1.

## Command Default

Displays predictive analytics of the top 1 percent multicast entries.

## Command Modes

Any command mode

## Command History

Release	Modification
Cisco NX-OS Release 8.2(1)	This command was introduced.

## Usage Guidelines

To view predictive analytics of multicast entries, you must enable Intelligent CAM (iCAM) monitoring on the corresponding entries using the **icam monitor entries** command.

## Examples

This example displays predictive analytics of multicast entries:

```
switch# show icam prediction entries multicast module 3 2020 Jul 19 08:10:29
Generating predictions, this may take some time ...
```

```
=====
Multicast Entries Prediction (Mod 3)
-----
-----
VDC_ID      TABLE_ID      Source/Mask      Group/Mask      RPF
Stats      Prediction
```

## show icam prediction entries multicast

```

-----
1          1  209.165.202.129/27      209.165.200.225/27  Ethernet3/12
1679387   1679387
1          1  209.165.201.23/27      209.165.200.225/27  Ethernet3/12
1679419   1679419
1          1  209.165.201.24/27      209.165.200.225/27  Ethernet3/12
1679411   1679411
1          1  209.165.201.25/27      209.165.200.225/27  Ethernet3/12
1679411   1679411
1          1  209.165.201.26/27      209.165.200.225/27  Ethernet3/12
1679411   1679411
1          1  209.165.201.27/27      209.165.200.225/27  Ethernet3/12
1679411   1679411
1          1  209.165.201.28/27      209.165.200.225/27  Ethernet3/12
1679404   1679404
1          1  209.165.201.29/27      209.165.200.225/27  Ethernet3/12
1679403   1679403
1          1  209.165.201.30/27      209.165.200.225/27  Ethernet3/12
1679403   1679403
1          1  209.165.201.8/27       209.165.200.225/27  Ethernet3/12
1679113   1679113
1          1  209.165.201.7/27       209.165.200.225/27  Ethernet3/12
1679113   1679113
1          1  209.165.201.4/27       209.165.200.225/27  Ethernet3/12
1679141   1679141
1          1  209.165.201.3/27       209.165.200.225/27  Ethernet3/12
1679142   1679142
1          1  209.165.201.6/27       209.165.200.225/27  Ethernet3/12
1679113   1679113
1          1  209.165.201.5/27       209.165.200.225/27  Ethernet3/12
1679141   1679141
1          1  209.165.200.238/27     209.165.200.225/27  Ethernet3/12
1679150   1679150
1          1  209.165.200.237/27     209.165.200.225/27  Ethernet3/12
1679150   1679150
1          1  209.165.201.2/27       209.165.200.225/27  Ethernet3/12
1679150   1679150
1          1  209.165.201.1/27       209.165.200.225/27  Ethernet3/12
1679150   1679150
1          1  209.165.200.226/27     209.165.200.225/27  Ethernet3/12
1679166   1679166
1          1  209.165.201.22/27      209.165.200.225/27  Ethernet3/12
1679422   1679422
1          1  209.165.201.21/27      209.165.200.225/27  Ethernet3/12
1679424   1679424
1          1  209.165.201.20/27      209.165.200.225/27  Ethernet3/12
1679424   1679424
1          1  209.165.201.19/27      209.165.200.225/27  Ethernet3/12
1679425   1679425
1          1  209.165.201.18/27      209.165.200.225/27  Ethernet3/12
1679431   1679431
1          1  209.165.201.17/27      209.165.200.225/27  Ethernet3/12
1679435   1679435
1          1  209.165.201.16/27      209.165.200.225/27  Ethernet3/12
1679438   1679438
1          1  209.165.201.15/27      209.165.200.225/27  Ethernet3/12
1679438   1679438
1          1  209.165.201.14/27      209.165.200.225/27  Ethernet3/12
1679443   1679443
1          1  209.165.201.13/27      209.165.200.225/27  Ethernet3/12
1679445   1679445
1          1  209.165.200.235/27     209.165.200.225/27  Ethernet3/12
1679150   1679150

```

```

1          1  209.165.200.236/27    209.165.200.225/27  Ethernet3/12
1679150    1679150
1          1  209.165.200.233/27    209.165.200.225/27  Ethernet3/12
1679165    1679165
1          1  209.165.200.234/27    209.165.200.225/27  Ethernet3/12
1679151    1679151
1          1  209.165.200.231/27    209.165.200.225/27  Ethernet3/12
1679165    1679165
1          1  209.165.200.232/27    209.165.200.225/27  Ethernet3/12
1679165    1679165
1          1  209.165.200.229/27    209.165.200.225/27  Ethernet3/12
1679165    1679165
1          1  209.165.200.230/27    209.165.200.225/27  Ethernet3/12
1679165    1679165
1          1  209.165.200.227/27    209.165.200.225/27  Ethernet3/12
1679166    1679166
1          1  209.165.200.228/27    209.165.200.225/27  Ethernet3/12
1679166    1679166
1          1  209.165.201.12/27     209.165.200.225/27  Ethernet3/12
1679103    1679103
1          1  209.165.201.9/27      209.165.200.225/27  Ethernet3/12
1679112    1679112
1          1  209.165.201.10/27     209.165.200.225/27  Ethernet3/12
1679113    1679113
1          1  209.165.201.11/27     209.165.200.225/27  Ethernet3/12
1679113    1679113
.
.
.

```

This example displays predictive analytics of the top 1 percent multicast entries:

```

switch# show icam prediction entries multicast module 3 2020 Jul 19 08:10:29 top 1
Generating predictions, this may take some time ...

```

```

=====
Multicast Entries Prediction (Mod 3)
-----

```

VDC_ID	TABLE_ID	Source/Mask	Group/Mask	RPF
Stats	Prediction			
1	1	209.165.202.129/27	209.165.200.225/27	Ethernet3/12
1679387	1679387			
1	1	209.165.201.23/27	209.165.200.225/27	Ethernet3/12
1679419	1679419			
1	1	209.165.201.24/27	209.165.200.225/27	Ethernet3/12
1679411	1679411			
1	1	209.165.201.25/27	209.165.200.225/27	Ethernet3/12
1679411	1679411			
1	1	209.165.201.26/27	209.165.200.225/27	Ethernet3/12
1679411	1679411			
1	1	209.165.201.27/27	209.165.200.225/27	Ethernet3/12
1679411	1679411			
1	1	209.165.201.28/27	209.165.200.225/27	Ethernet3/12
1679404	1679404			
1	1	209.165.201.29/27	209.165.200.225/27	Ethernet3/12
1679403	1679403			
1	1	209.165.201.30/27	209.165.200.225/27	Ethernet3/12
1679403	1679403			

## show icam prediction entries multicast

```

1          1      209.165.201.8/27      209.165.200.225/27  Ethernet3/12
1679113   1679113
1          1      209.165.201.7/27      209.165.200.225/27  Ethernet3/12
1679113   1679113
1          1      209.165.201.4/27      209.165.200.225/27  Ethernet3/12
1679141   1679141
1          1      209.165.201.3/27      209.165.200.225/27  Ethernet3/12
1679142   1679142
1          1      209.165.201.6/27      209.165.200.225/27  Ethernet3/12
1679113   1679113
1          1      209.165.201.5/27      209.165.200.225/27  Ethernet3/12
1679141   1679141
1          1      209.165.200.238/27    209.165.200.225/27  Ethernet3/12
1679150   1679150
1          1      209.165.200.237/27    209.165.200.225/27  Ethernet3/12
1679150   1679150
1          1      209.165.201.2/27     209.165.200.225/27  Ethernet3/12
1679150   1679150
1          1      209.165.201.1/27     209.165.200.225/27  Ethernet3/12
1679150   1679150
1          1      209.165.200.226/27    209.165.200.225/27  Ethernet3/12
1679166   1679166
1          1      209.165.201.22/27    209.165.200.225/27  Ethernet3/12
1679422   1679422
1          1      209.165.201.21/27    209.165.200.225/27  Ethernet3/12
1679424   1679424
1          1      209.165.201.20/27    209.165.200.225/27  Ethernet3/12
1679424   1679424
1          1      209.165.201.19/27    209.165.200.225/27  Ethernet3/12
1679425   1679425
1          1      209.165.201.18/27    209.165.200.225/27  Ethernet3/12
1679431   1679431
1          1      209.165.201.17/27    209.165.200.225/27  Ethernet3/12
1679435   1679435
1          1      209.165.201.16/27    209.165.200.225/27  Ethernet3/12
1679438   1679438
1          1      209.165.201.15/27    209.165.200.225/27  Ethernet3/12
1679438   1679438
1          1      209.165.201.14/27    209.165.200.225/27  Ethernet3/12
1679443   1679443
1          1      209.165.201.13/27    209.165.200.225/27  Ethernet3/12
1679445   1679445
1          1      209.165.200.235/27    209.165.200.225/27  Ethernet3/12
1679150   1679150
1          1      209.165.200.236/27    209.165.200.225/27  Ethernet3/12
1679150   1679150
1          1      209.165.200.233/27    209.165.200.225/27  Ethernet3/12
1679165   1679165
1          1      209.165.200.234/27    209.165.200.225/27  Ethernet3/12
1679151   1679151
1          1      209.165.200.231/27    209.165.200.225/27  Ethernet3/12
1679165   1679165
1          1      209.165.200.232/27    209.165.200.225/27  Ethernet3/12
1679165   1679165
1          1      209.165.200.229/27    209.165.200.225/27  Ethernet3/12
1679165   1679165
1          1      209.165.200.230/27    209.165.200.225/27  Ethernet3/12
1679165   1679165
1          1      209.165.200.227/27    209.165.200.225/27  Ethernet3/12
1679166   1679166
1          1      209.165.200.228/27    209.165.200.225/27  Ethernet3/12
1679166   1679166
1          1      209.165.201.12/27    209.165.200.225/27  Ethernet3/12
1679103   1679103

```

```

1          1      209.165.201.9/27      209.165.200.225/27  Ethernet3/12
1679112   1679112
1          1      209.165.201.10/27     209.165.200.225/27  Ethernet3/12
1679113   1679113
1          1      209.165.201.11/27    209.165.200.225/27  Ethernet3/12
1679113   1679113
.
.
.

```

**Related Commands**

Command	Description
<b>feature icam</b>	Enables the iCAM feature.
<b>icam monitor entries</b>	Enables iCAM monitoring on TCAM entries.
<b>icam monitor interval</b>	Configures the iCAM monitor interval and the number of intervals in an iCAM monitor history.
<b>icam monitor resource</b>	Enables iCAM monitoring on TCAM resources.
<b>show icam entries acl</b>	Displays traffic analytics of the ACL TCAM, which includes RACL, VACL, QoS, PBR, WCCP, CoPP, and so on.
<b>show icam entries multicast</b>	Displays traffic analytics of multicast entries.
<b>show icam prediction entries acl</b>	Displays machine-learning predictive analytics of TCAM entries.
<b>show icam prediction resource</b>	Displays machine-learning predictive analytics of TCAM resource utilization.
<b>show icam resource</b>	Displays TCAM resource utilization.

# show icam prediction resource

To display machine-learning predictive analytics of ternary content addressable memory (TCAM) resource utilization, use the **show icam prediction resource** command.

```
show icam prediction resource {acl_tcam | fib_tcam} module module inst instance year month
day time
```

Syntax Description	Parameter	Description
	<b>acl_tcam</b>	Specifies access control list (ACL) TCAM resources.
	<b>module</b> <i>module</i>	Specifies the module number. The range is from 1–18 for an 18-slot chassis, and from 1–9 for a 9-slot chassis.
	<b>inst</b> <i>instance</i>	Specifies the ASIC or forwarding engine instance number. The range is from 0–11.
	<b>fib_tcam</b>	Specifies forwarding information base (FIB) TCAM resources.
	<i>year</i>	Year in YYYY format. The values range from 1970–2030.
	<i>month</i>	Month in MMM format, for example, Jan, Feb, and so on. The values are case sensitive.
	<i>day</i>	Day of the month in DD format. The range is from 1–31.
	<i>time</i>	Time in HH:MM:SS format.

**Command Default** None

**Command Modes** Any command mode

Command History	Release	Modification
	Cisco NX-OS Release 8.2(1)	This command was introduced.

**Usage Guidelines** To view predictive analytics of TCAM resource utilization, you must enable iCAM monitoring on the required resources using the **icam monitor resource** command.

**Examples** This example shows how to view predictive analytics of ACL TCAM resource utilization:

```
switch# show icam prediction resource acl_tcam module 3 inst 4 2018 Jan 27 11:35:30
Generating predictions, this may take some time ...
-----
---
Feature Hardware Resource Prediction (Mod 3,Inst 4)
-----
---
-----
---
          Feature   Direction   TCAM#   BANK#   Feature_Entries   Free_Entries
Percent_Util
```

```

-----
---
          PACL      ingress      0      0      4      4072
0.00
          FEX Control ingress      1      0      5      4071
0.00
          CoPP      ingress      1      1      420     3656
10.00

=====
===
ACL TCAM Resource Prediction (Mod 3,Inst 4)
-----
---
          Used      Free      Percent_Util
-----
---
Tcam 1 Bank 1      440     3656          10.74
Tcam 1 Bank 0       25     4071           0.61
Tcam 0 Bank 1       20     4076           0.48
Tcam 0 Bank 0       24     4072           0.58

```

This example shows how to view predictive analytics of FIB TCAM resource utilization:

```
switch# show icam prediction resource fib_tcam module 3 inst 5 2025 Dec 20 10:20:37
```

Generating predictions, this may take some time ...

```

=====
FIB TCAM Resource Prediction (Mod 3, Inst 5)
-----
-----
          Type      logical      physical      Percent_Util
-----
          FC MPLS      0           0           0.00
          IPV4 unicast 16          16          0.00
          DIAG_80      1           1           0.00
          EOM Peer     0           0           0.00
          MPLS         0           0           0.00
          IPV6 multicast 5           20          0.00
          IPV6 LinkLocal 1           2           0.00
          FCOE         0           0           0.00
          MPLS VPN     0           0           0.00
          IPV4 multicast 5005        5005        7.00
          IPV6 unicast 4           8           0.00

```

## Related Commands

Command	Description
<b>feature icam</b>	Enables the iCAM feature.
<b>icam monitor entries</b>	Enables iCAM monitoring on TCAM entries.
<b>icam monitor interval</b>	Configures the iCAM monitor interval and the number of intervals in an iCAM monitor history.
<b>icam monitor resource</b>	Enables iCAM monitoring on TCAM resources.
<b>show icam entries acl</b>	Displays traffic analytics of the ACL TCAM, which includes RACL, VACL, QoS, PBR, WCCP, CoPP, and so on.
<b>show icam entries multicast</b>	Displays traffic analytics of multicast entries.

Command	Description
<b>show icam prediction entries acl</b>	Displays machine-learning predictive analytics of TCAM entries.
<b>show icam prediction entries multicast</b>	Displays machine-learning predictive analytics of multicast entries.
<b>show icam resource</b>	Displays TCAM resource utilization.



# show icam resource

To display ternary content addressable memory (TCAM) resource utilization, use the **show icam resource** command.

```
show icam resource {acl_tcam | fib_tcam} module module inst instance [history num-intervals]
```

Syntax Description		
<b>acl_tcam</b>		Specifies access control list (ACL) TCAM resources.
<b>module</b> <i>module</i>		Specifies the module number. The range is from 1–18 for an 18-slot chassis, and from 1–9 for a 9-slot chassis.
<b>inst</b> <i>instance</i>		Specifies the ASIC or forwarding engine instance number. The range is from 0–11.
<b>fib_tcam</b>		Specifies forwarding information base (FIB) TCAM resources.
<b>history</b>		(Optional) Shows resource history.
<i>num-intervals</i>		Number of intervals in history. The range is from 168–1344.

**Command Default** None

**Command Modes** Any command mode

Command History	Release	Modification
	Cisco NX-OS Release 8.2(1)	This command was modified. The following keywords and arguments were added: <ul style="list-style-type: none"> <li>• <b>acl_tcam</b></li> <li>• <b>fib_tcam</b></li> <li>• <b>history num-intervals</b></li> </ul>
	Cisco NX-OS Release 8.0(1)	This command was introduced.

**Usage Guidelines** To view the history of TCAM resource utilization, you must enable Intelligent CAM (iCAM) monitoring on the corresponding resources using the **icam monitor resource** command.

**Examples** This example shows how to view ACL TCAM resource utilization:

```
switch# show icam resource acl_tcam module 3 inst 5
-----
---
Feature Hardware Resource Utilization (Mod 3,Inst 5)
-----
---

Ingress Resources
```

## show icam resource

```

-----
---
      Feature TCAM# BANK# Feature_Entries  Free_Entries  Percent_Util  Timestamp
(UTC)
-----
---
      RACL      1      0           6           4065           0.14 2017-09-05
22:05:52
      CoPP      1      1          420          3656           10.25 2017-09-05
22:05:52
      FEX Control  1      0           5           4065           0.12 2017-09-05
22:05:52

Egress Resources
-----
---
      Feature TCAM# BANK# Feature_Entries  Free_Entries  Percent_Util  Timestamp
(UTC)
-----
---
=====
===
ACL TCAM Resource Utilization (Mod 3,Inst 5)
-----
---
              Used    Free    Percent_Util          Timestamp (UTC)
-----
---
Tcam 0 Bank 0      20    4076           0.48    2017-09-05 22:05:52
Tcam 0 Bank 1      20    4076           0.48    2017-09-05 22:05:52
Tcam 1 Bank 0      31    4065           0.75    2017-09-05 22:05:52
Tcam 1 Bank 1     440    3656           10.74    2017-09-05 22:05:52

```

This example shows how to view the history of ACL TCAM resource utilization:

```
switch# show icam resource acl_tcam module 3 inst 5 history 2
```

```

-----
---
Feature Hardware Resource Utilization (Mod 3,Inst 5)
-----
---

Ingress Resources
-----
---
      Feature TCAM# BANK# Feature_Entries  Free_Entries  Percent_Util  Timestamp
(UTC)
-----
---
      RACL      1      0           6           4065           0.14 2017-09-05
22:13:13
              6           4065           0.14 2017-09-05
23:13:13
      CoPP      1      1          420          3656           10.25 2017-09-05
22:13:13
              420          3656           10.25 2017-09-05
23:13:13
      FEX Control  1      0           5           4065           0.12 2017-09-05
22:13:13

```

```

23:13:13                    5          4065          0.12 2017-09-05

Egress Resources
-----
---
      Feature TCAM# BANK# Feature_Entries  Free_Entries  Percent_Util  Timestamp
(UTC)
-----
---
=====
===
ACL TCAM Resource Utilization (Mod 3,Inst 5)
-----
---
              Used    Free    Percent_Util          Timestamp (UTC)
-----
---
Tcam 0 Bank 0      20   4076         0.48    2017-09-05 22:13:13
                  20   4076         0.48    2017-09-05 23:13:13
Tcam 0 Bank 1      20   4076         0.48    2017-09-05 22:13:13
                  20   4076         0.48    2017-09-05 23:13:13
Tcam 1 Bank 0      31   4065         0.75    2017-09-05 22:13:13
                  31   4065         0.75    2017-09-05 23:13:13
Tcam 1 Bank 1     440  3656        10.74    2017-09-05 22:13:13
                  440  3656        10.74    2017-09-05 23:13:13

```

This example shows how to view FIB TCAM resource utilization:

```

switch# show icam resource fib_tcam module 3 inst 5

=====
FIB TCAM Resource Utilization (Mod 3, Inst 5)
-----
-----
      Type          logical    physical  Percent_Util  Timestamp (UTC)
-----
IPV4 unicast          16         16         0.02    2017-09-05 22:09:19
      DIAG_80          1          1          0.00    2017-09-05 22:09:19
IPV4 multicast        5005       5005         7.82    2017-09-05 22:09:19
      MPLS              0          0          0.00    2017-09-05 22:09:19
      EOM Peer          0          0          0.00    2017-09-05 22:09:19
      MPLS VPN          0          0          0.00    2017-09-05 22:09:19
      FCMPLS            0          0          0.00    2017-09-05 22:09:19
      FCOE              0          0          0.00    2017-09-05 22:09:19
IPV6 LinkLocal        1          2          0.00    2017-09-05 22:09:19
      IPV6 unicast      4          8          0.01    2017-09-05 22:09:19
      IPV6 multicast    5          20         0.03    2017-09-05 22:09:19

```

This example shows how to view the history of FIB TCAM resource utilization:

```

switch# show icam resource fib_tcam module 3 inst 5 history 2

=====
FIB TCAM Resource Utilization (Mod 3, Inst 5)
-----
-----
      Type          logical    physical  Percent_Util  Timestamp (UTC)
-----
IPV4 unicast          16         16         0.02    2017-09-05 22:17:14
                  16         16         0.02    2017-09-05 23:17:14
      DIAG_80          1          1          0.00    2017-09-05 22:17:14

```

## show icam resource

	1	1	0.00	2017-09-05 23:17:14
IPV4 multicast	5005	5005	7.82	2017-09-05 22:17:14
	5005	5005	7.82	2017-09-05 23:17:14
MPLS	0	0	0.00	2017-09-05 22:17:14
	0	0	0.00	2017-09-05 23:17:14
EOM Peer	0	0	0.00	2017-09-05 22:17:14
	0	0	0.00	2017-09-05 23:17:14
MPLS VPN	0	0	0.00	2017-09-05 22:17:14
	0	0	0.00	2017-09-05 23:17:14
FCMPLS	0	0	0.00	2017-09-05 22:17:14
	0	0	0.00	2017-09-05 23:17:14
FCOE	0	0	0.00	2017-09-05 22:17:14
	0	0	0.00	2017-09-05 23:17:14
IPV6 LinkLocal	1	2	0.00	2017-09-05 22:17:14
	1	2	0.00	2017-09-05 23:17:14
IPV6 unicast	4	8	0.01	2017-09-05 22:17:14
	4	8	0.01	2017-09-05 23:17:14
IPV6 multicast	5	20	0.03	2017-09-05 22:17:14
	5	20	0.03	2017-09-05 23:17:14

## Related Commands

Command	Description
<b>feature icam</b>	Enables the iCAM feature.
<b>icam monitor entries</b>	Enables iCAM monitoring on TCAM entries.
<b>icam monitor interval</b>	Configures the iCAM monitor interval and the number of intervals in an iCAM monitor history.
<b>icam monitor resource</b>	Enables iCAM monitoring on TCAM resources.
<b>show icam entries acl</b>	Displays traffic analytics of the ACL TCAM, which includes RACL, VACL, QoS, PBR, WCCP, CoPP, and so on.
<b>show icam entries multicast</b>	Displays the traffic analytics of multicast entries.
<b>show icam prediction entries acl</b>	Displays machine-learning predictive analytics of TCAM entries.
<b>show icam prediction entries multicast</b>	Displays machine-learning predictive analytics of multicast entries.
<b>show icam prediction resource</b>	Displays the machine-learning predictive analytics of TCAM resource utilization.

# show interface ethernet capabilities

To show if an interface is Energy Efficient Ethernet (EEE) capable, use the **show interface ethernet capabilities** command.

**show interface ethernet *slot/chassis* capabilities**

<b>Syntax Description</b>	<i>slot/chassis</i>	Slot or chassis number. The range is from 1 to 253.
	<b>capabilities</b>	(Optional) Displays clock module information.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		6.1(2)

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

**Examples**

This example shows how to display if an interface is EEE capable:

```
switch(config-if)# show interface ethernet 16/1 capabilities
Ethernet16/1
  Model: N7K-F248XT-25
  Type (Non SFP): 10g
  Speed: 1000,10000
  Duplex: full
  Trunk encap. type: 802.1Q
  FabricPath capable: yes
  Channel: yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol: rx-(off/on/desired),tx-(off/on/desired)
  Rate mode: dedicated
  Port mode: Routed,Switched
  QOS scheduling: rx-(8q4t),tx-(3p5q1t)
  CoS rewrite: yes
  ToS rewrite: yes
  SPAN: yes
  UDLD: yes
  MDIX: yes
  TDR capable: yes
  Link Debounce: yes
  Link Debounce Time: yes
  FEX Fabric: yes
  dot1Q-tunnel mode: yes
  Pvlan Trunk capable: yes
  Port Group Members: 1-4
  EEE (efficient-eth): yes
  PFC capable: yes
switch(config-if)#
```

# show interface ethernet

To display the Energy Efficient Ethernet (EEE) status on an interface, Use the **show interface** command.

**show interface ethernet** *slot/chassis*

<b>Syntax Description</b>	<i>slot/chassis</i>	Slot or chassis number. The range is from 1 to 253.
---------------------------	---------------------	---

<b>Defaults</b>	None.
-----------------	-------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	6.1(2)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display the EEE status on an interface:

```
switch# show interface ethernet2/6
Ethernet2/6 is down (Link not connected)
admin state is up, Dedicated Interface
  Hardware: 10000 Ethernet, address: 0022.5579.de41 (bia 001b.54c1.af5d)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  auto-duplex, auto-speed, media type is 10G
  Beacon is turned off
  Auto-Negotiation is turned off
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  Rate mode is shared
  Switchport monitor is off
  EtherType is 0x8100
  EEE (efficient-ethernet) : n/a
  Last link flapped never
  Last clearing of "show interface" counters never
  0 interface resets
  30 seconds input rate 0 bits/sec, 0 packets/sec
  30 seconds output rate 0 bits/sec, 0 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
```

## ■ show interface ethernet

```
input rate 0 bps, 0 pps; output rate 0 bps, 0 pps
L3 in Switched:
  ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
--More--
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show lldp tlv-select</b>	Displays the LLDP TLV configuration.
<b>lldp tlv-select</b>	Specifies the TLVs to send and receive in LLDP packets.



# show interface ethernet counter detailed

To display the only nonzero counters, use the **show interface ethernet counter detailed** command.

**show interface ethernet *slot/chassis* counter detailed**

<b>Syntax Description</b>	<i>slot/chassis</i>	Slot or chassis number. The range is from 1 to 253.
---------------------------	---------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	6.1(2)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display the only nonzero counters:

```
switch# show interface ethernet 10/25 counters detailed
Ethernet10/25
Rx Packets:                               3635
  Rx Unicast Packets:                     9788
  Rx Multicast Packets:                   3631
Rx Bytes:                                  1062103
  Rx Packets from 128 to 255 bytes:       1211
  Rx Packets from 256 to 511 bytes:       2420
  Rx Packets from 1024 to 1518 bytes:     4
Tx Packets:                                39883
  Tx Unicast Packets:                     9788
  Tx Multicast Packets:                   39879
Tx Bytes:                                   3731578
  Tx Packets from 65 to 127 bytes:        36247
  Tx Packets from 128 to 255 bytes:       1211
  Tx Packets from 256 to 511 bytes:       2421
  Tx Packets from 1024 to 1518 bytes:     4
Non Fcoe in packets:                      13419
Non Fcoe in octets:                       2392727
Non Fcoe out packets:                     39883
Non Fcoe out octets:                      3731578
Tx LPI uses                               74304694529
```

## ■ show interface ethernet counter detailed

```
Rx LPI usecs                74329358769
Tx LPI requests             39865
Rx LPI indications         3628
switch(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show lldp tlv-select</b>	Displays the LLDP TLV configuration.
<b>lldp tlv-select</b>	Specifies the TLVs to send and receive in LLDP packets.

# show inventory

To display inventory information for the device hardware, use the **show inventory** command.

**show inventory** [**chassis** | **clock** | **fans** | **module** | **power\_supply**]

Syntax Description	
<b>chassis</b>	(Optional) Displays chassis information.
<b>clock</b>	(Optional) Displays clock module information.
<b>fans</b>	(Optional) Displays fan information.
<b>module</b>	(Optional) Displays module information.
<b>power_supply</b>	(Optional) Displays power supply information.

**Defaults** Displays all hardware inventory information.

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples**

This example shows how to display configuration incompatibilities:

```
switch# show inventory
NAME: "Chassis", DESCR: "Nexus7000 C7010 (10 Slot) Chassis "
PID: N7K-C7010 , VID: , SN: TBM11256507

NAME: "Slot 2", DESCR: "10/100/1000 Mbps Ethernet Module"
PID: N7K-M148GT-11 , VID: , SN: JAB104400P0

NAME: "Slot 6", DESCR: "Supervisor module-1X"
PID: N7K-SUP1 , VID: TBD , SN: JAB10380101

NAME: "Slot 11", DESCR: "Fabric card module"
PID: N7K-C7010-FAB-1 , VID: , SN: JAB104300HM

NAME: "Slot 33", DESCR: "Nexus7000 C7010 (10 Slot) Chassis Power Supply"
PID: FIORANO , VID: , SN: DTH1117T005

NAME: "Slot 34", DESCR: "Nexus7000 C7010 (10 Slot) Chassis Power Supply"
PID: N7K-AC-6.0KW , VID: , SN: DTH1117T009

NAME: "Slot 36", DESCR: "Nexus7000 C7010 (10 Slot) Chassis Fan Module"
PID: , VID: V00, SN:

NAME: "Slot 37", DESCR: "Nexus7000 C7010 (10 Slot) Chassis Fan Module"
PID: , VID: V00, SN:

NAME: "Slot 38", DESCR: "Nexus7000 C7010 (10 Slot) Chassis Fan Module"
PID: , VID: V00, SN:

NAME: "Slot 39", DESCR: "Nexus7000 C7010 (10 Slot) Chassis Fan Module"
PID: , VID: V00, SN:

switch#
```

# show lldp dcbx interface ethernet

To display the local Data Center Bridging Capability Exchange (DCBX) control status of an interface, use the **show lldp dcbx interface ethernet** command.

**show lldp dcbx interface ethernet** *slot/port-number*

<b>Syntax Description</b>	<i>slot/port-number</i> Slot number and port number is in this format: <i>slot/port-number</i> . The range is from 1 to 253.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display the local DCBX control status:

```
switch(config)# show lldp dcbx interface ethernet 1/5
Local DCBXP Control information:
Operation version: 00 Max version: 00 Seq no: 1 Ack no: 1 Type/
Subtype Version En/Will/Adv Config
003/000 000 Y/N/Y 0008
002/000 000 Y/N/Y 1111100032 32000000 00000002

Peer's DCBXP Control information:
Operation version: 00 Max version: 00 Seq no: 1 Ack no: 1
Type/ Max/Oper
Subtype Version En/Will/Err Config
003/000 000/000 Y/N/N 0008
002/000 000/000 Y/N/N 1111100032 32000000 00000002

switch(config)#
```

## ■ show lldp dcbx interface ethernet

Related Commands	Command	Description
	show lldp tlv-select	Displays the LLDP TLV configuration.
	lldp tlv-select	Specifies the TLVs to send and receive in LLDP packets.

# show lldp interface ethernet

To display the Link Layer Discovery Protocol (LLDP) configuration on the interface, use the **show lldp interface ethernet** command.

**show lldp interface ethernet** *slot/port-number*

<b>Syntax Description</b>	<i>slot/port-number</i> Slot number and port number in this format: <i>slot/port-number</i> . The range is from 1 to 253.										
<b>Defaults</b>	None										
<b>Command Modes</b>	Any command mode										
<b>Supported User Roles</b>	network-admin network-operator vdc-admin vdc-operator										
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>5.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	5.0(1)	This command was introduced.						
Release	Modification										
5.0(1)	This command was introduced.										
<b>Usage Guidelines</b>	This command does not require a license.										
<b>Examples</b>	<p>This example shows how to display the LLDP configuration on the interface:</p> <pre>switch(config)# show lldp interface ethernet 6/3 Interface Information:   Enable (tx/rx/dcbx): Y/Y/Y    Port Mac address: 00:24:f7:19:84:72 switch(config)#</pre>										
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show lldp traffic interface ethernet</b></td> <td>Displays the number of LLDP packets sent and received on the interface.</td> </tr> <tr> <td><b>show running-config lldp</b></td> <td>Displays the global LLDP configuration.</td> </tr> <tr> <td><b>lldp transmit</b></td> <td>Enables the transmission of LLDP packets on an interface.</td> </tr> <tr> <td><b>lldp receive</b></td> <td>Enables the reception of LLDP packets on an interface.</td> </tr> </tbody> </table>	Command	Description	<b>show lldp traffic interface ethernet</b>	Displays the number of LLDP packets sent and received on the interface.	<b>show running-config lldp</b>	Displays the global LLDP configuration.	<b>lldp transmit</b>	Enables the transmission of LLDP packets on an interface.	<b>lldp receive</b>	Enables the reception of LLDP packets on an interface.
Command	Description										
<b>show lldp traffic interface ethernet</b>	Displays the number of LLDP packets sent and received on the interface.										
<b>show running-config lldp</b>	Displays the global LLDP configuration.										
<b>lldp transmit</b>	Enables the transmission of LLDP packets on an interface.										
<b>lldp receive</b>	Enables the reception of LLDP packets on an interface.										

# show lldp neighbors

To display the status of the Link Layer Discovery Protocol (LLDP) neighbor device, use the **show lldp neighbors** command.

```
show lldp neighbors {detail | interface ethernet slot/port-number}
```

Syntax Description	detail	Displays LLDP neighbor detail information.
	<b>interface ethernet</b>	Specifies the interface for which you are displaying LLDP information.
	<i>slot/port-number</i>	Slot number and port number in this format: <i>slot/port-number</i> . The range is from 1 to 253.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
vdc-admin  
network-operator  
vdc-operator

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

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

**Examples** This example shows how to display the LLDP neighbor device status:

```
switch(config)# show lldp neighbors detail
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Local Intf Chassis ID Port ID Hold-time Capability
Eth8/24 0018.bad8.5e45 Eth8/23 120 R
Eth8/23 0018.bad8.5e45 Eth8/24 120 R
switch(config)#
```



Related Commands	Command	Description
	<b>show lldp traffic</b>	Displays the LLDP counters, including the number of LLDP packets sent and received by the device, the number of discarded packets, and the number of unrecognized TLVs.
	<b>show lldp traffic interface ethernet</b>	Displays the number of LLDP packets sent and received on the interface.

# show lldp timers

To display the Link Layer Discovery Protocol (LLDP) hold time, delay time, and update frequency configuration, use the **show lldp timers** command.

## show lldp timers

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the LLDP hold time, delay time, and update frequency configuration:

```
switch(config)# show lldp timers
LLDP Timers:

    Holdtime in seconds: 180
    Reinit-time in seconds: 6
    Transmit interval in seconds: 45
switch(config)#
```

Related Commands	Command	Description
	<b>show lldp holdtime</b>	Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.
	<b>lldp reinit</b>	Specifies the delay time in seconds for LLDP to initialize on any interface.
	<b>lldp timer</b>	Specifies the transmission frequency of LLDP updates in seconds.

# show lldp tlv-select

To display the type, length, and value (TLV) configuration for the Link Layer Discovery Protocol (LLDP), use the **show lldp tlv-select** command.

**show lldp tlv-select**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the TLV configuration for LLDP:

```
switch(config)# show lldp tlv-select
  access-management
  dcbx
  port-description
  port-vlan
  system-capabilities
  system-description
  system-name

switch(config)#
```

Related Commands	Command	Description
	<b>show lldp dcbx interface ethernet</b>	Displays the local DCBX control status.
	<b>lldp tlv-select</b>	Specifies the TLVs to send and receive in LLDP packets.

# show lldp traffic

To display the Link Layer Discovery Protocol (LLDP) counters, including the number of LLDP packets sent and received by the device, the number of discarded packets, and the number of unrecognized TLVs, use the **show lldp traffic** command.

## show lldp traffic

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the LLDP counters:

```
switch(config)# show lldp traffic
LLDP traffic statistics:

    Total frames transmitted: 323
    Total entries aged: 0
    Total frames received: 0
    Total frames received in error: 0
    Total frames discarded: 0
    Total unrecognized TLVs: 0
switch(config)#
```

Related Commands	Command	Description
	<b>show lldp traffic interface ethernet</b>	Displays the number of LLDP packets sent and received on the interface.
	<b>show running-config lldp</b>	Displays the global LLDP configuration.

# show lldp traffic interface ethernet

To display the number of Link Layer Discovery Protocol (LLDP) packets sent and received on the interface, use the **show lldp traffic interface ethernet** command.

**show lldp traffic interface ethernet** *slot/port-number*

<b>Syntax Description</b>	<i>slot/port-number</i> Slot number and port number in this format: <i>slot/port-number</i> . The range is from 1 to 253.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>Supported User Roles</b>	network-admin network-operator vdc-admin vdc-operator
-----------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display the number of LLDP packets sent and received on the interface:
-----------------	--

```
switch(config)# show lldp traffic interface ethernet 7/1
LLDP interface traffic statistics:

    Total frames transmitted: 0
    Total entries aged: 0
    Total frames received: 0
    Total frames received in error: 0
    Total frames discarded: 0
    Total unrecognized TLVs: 0
switch(config)#
```

Related Commands	Command	Description
	<b>show lldp traffic</b>	Displays the LLDP counters, including the number of LLDP packets sent and received by the device, the number of discarded packets, and the number of unrecognized TLVs.
	<b>show running-config lldp</b>	Displays the global LLDP configuration.

# show locator-led status

To show the status of locator LEDs on the system, use the **show locator-led status** command.

## show locator-led status

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows the locator LED status for the system:

```
switch# show locator-led status
Xbar 1 : Locator LED off
Module 7 : Locator LED off
Module 9 : Locator LED off
Module 12 is not powered up.
Chassis Locator LED off
PowerSupply 1 : Locator LED off
PowerSupply 2 : Locator LED off
Fan 1 : Locator LED off
Fan 2 : Locator LED off
switch(config)#
```

Related Commands	Command	Description
	locator-led	Blinks an LED on the system.

# 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.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the console logging configuration:

```
switch# show logging console
Logging console:          enabled (Severity: critical)
switch#
```

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



# 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.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

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

**Examples**

This example shows how to display the logging configuration:

```
switch# show logging info
Logging console:          enabled (Severity: critical)
Logging monitor:         enabled (Severity: notifications)
Logging linecard:        enabled (Severity: notifications)
Logging timestamp:       Seconds
Logging loopback :       disabled
Logging server:          enabled
{172.28.254.254}
    server severity:      notifications
    server facility:      local7
    server VRF:           default
Logging logflash:        enabled (Severity: information)
Logging logfile:         enabled
Name - messages: Severity - information Size - 10485760
```

Facility	Default Severity	Current Session Severity
-----	-----	-----
aaa	3	5
aclog	2	2
aclmgr	3	3
auth	0	0
authpriv	3	3
bfd	2	2
--More--		

# show logging ip access-list cache

To display information about the logging IP access list cache, use the **show logging ip access-list cache** command.

## show logging ip access-list cache

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	6.2(6)	This command was modified. The output was modified to include additional parameters if detailed IP access list logging is enabled.
	4.0(1)	This command was introduced.

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

When detailed logging is enabled, the following additional parameters will be displayed in ACL-LOG cache entry with the currently collected ACL-LOG fields:

- ACL Name
- ACE Number
- ACE Action (Permit /Deny)
- ACL Direction (Ingress/Egress)
- ACL Filter Type (RACL\_IPV4/PACL\_MAC/ PACL\_IPV4/PBR/VACL)
- ACL Applied Interface

**Examples** This example shows how to display information about the logging IP access list cache:

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

## ■ show logging ip access-list cache

Related Commands	Command	Description
	<b>logging ip access-list cache</b>	Configures Optimized ACL Logging (OAL) parameters.
	<b>logging ip access-list detailed</b>	Enables detailed logging for access lists.

# show logging last

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

**show logging last** *number*

<b>Syntax Description</b>	<i>number</i>	Number of lines. The range is from 1 to 9999.
---------------------------	---------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display the last 42 lines of the logfile:
-----------------	---

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

# show logging level

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

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

<b>Syntax Description</b>	<i>level</i>	(Optional) Logging configuration to display. The keyword options are listed in the <a href="#">“System Message Logging Facilities” section on page 1</a> .
---------------------------	--------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.
	4.0(2)	Added the <b>interface-vlan</b> , <b>netstack</b> , <b>private-vlan</b> , and <b>ipv6</b> keywords.
	4.1(2)	Added the <b>cfs</b> keyword.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display the current Cisco Fabric Services (CFS) logging configuration:
-----------------	--

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

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>logging level</b>	Configures the facility logging level.

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** If you do not enter an end time, the current time is used.  
This command does not require a license.

**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
switch#
```

Related Commands	Command	Description
	logging logfile	Configures logging to a log file.

# show logging loopback

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

**show logging loopback**

---

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

---

**Defaults** None

---

**Command Modes** Any command mode

---

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

---

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

---



---

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

---

**Examples** This example shows how to display the logging loopback configuration:

```
switch# show logging loopback
switch#
```



# 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.

---

**Defaults** None

---

**Command Modes** Any command mode

---

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

---

---

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

---

**Examples** This example shows how to display the module logging configuration:

```
switch# show logging module  
switch#
```

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>logging module</b>	Configures module logging.

---

# 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.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the monitor logging configuration:

```
switch# show logging monitor
switch#
```

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

# show logging nvram

To display the messages in the NVRAM log, use the **show logging nvram** command.

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

<b>Syntax Description</b>	<b>last</b> <i>number-lines</i> (Optional) Specifies a number of lines to display. The last <i>number-lines</i> is displayed. The range is from 1 to 100 lines.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>Supported User Roles</b>	network-admin network-operator vdc-admin vdc-operator
-----------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display the last 20 messages in the NVRAM log:
-----------------	--

```
switch# show logging nvram last 20
switch#
```

# show logging onboard

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

```
show logging onboard { boot-uptime | card-boot-history | card-first-power-on | cpuhog |
  credit-loss | counter-stats | device-version | endtime | environmental-history | error-stats |
  exception-log | flow-control | internal | interrupt-stats | kernel-trace | mem-leak |
  memory-errors | memory-info | module num | obfl-history | obfl-logs | register-log | rxwait
  | stack-trace | starttime | status | txwait }
```

## Syntax Description

<b>boot-uptime</b>	Displays the OBFL boot and uptime information.
<b>card-boot-history</b>	Displays the OBFL card boot history.
<b>card-first-power-on</b>	Displays the OBFL card first power on information.
<b>cpuhog</b>	Displays the OBFL information for CPU hog events.
<b>credit-loss</b>	Displays the OBFL credit loss logs.
<b>counter-stats</b>	(Optional) Displays the OBFL counter statistics.
<b>device-version</b>	Displays the OBFL device version information.
<b>endtime</b>	Displays the OBFL logs until the specified end time.
<b>environmental-history</b>	Displays the OBFL environmental history.
<b>error-stats</b>	Displays the OBFL error statistics.
<b>exception-log</b>	Displays the OBFL exception log.
<b>flow-control</b>	Displays the OBFL flow control logs.
<b>internal</b>	Displays the logging onboard internal information.
<b>interrupt-stats</b>	Displays the OBFL interrupt statistics.
<b>kernel-trace</b>	Displays the OBFL kernel trace information.
<b>mem-leak</b>	Displays the OBFL memory leak information.
<b>memory-errors</b>	Displays the memory error log for corrected single bit
<b>memory-info</b>	Displays memory information.
<b>module <i>num</i></b>	Displays the OBFL information for a specific module.
<b>obfl-history</b>	Displays the OBFL history information.
<b>obfl-logs</b>	Displays the OBFL tech support log information.
<b>register-log</b>	Displays the OBFL register log information.
<b>rxwait</b>	Displays the OBFL RxWait log information.
<b>stack-trace</b>	Displays the OBFL kernel stack trace information.
<b>starttime</b>	Displays the OBFL logs from the specified start time.
<b>status</b>	Displays the OBFL status enable/disable.
<b>txwait</b>	Displays the OBFL TxWait log information.

## Defaults

None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	8.2(1)	Added the <b>rxwait</b> and <b>txwait</b> keywords.
	4.0(2)	Added the <b>counter-stats</b> keyword.
	4.0(1)	This command was introduced.

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

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

The valid values for *file* are as follows:

- **bootflash:**
- **ftp:**
- **scp:**
- **sftp:**
- **slot0:**
- **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. The range is from 1 to 999.
  - **-B num**—Prints the specifies number of lines of context before every matching line. The range is from 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. The range is from 0 to 2147483647.
- **include [-i] [-x] [word]**—Includes the lines that match.
  - **-i**—Ignores the case difference when comparing the strings.
  - **-x**—Prints only the lines where the match is a whole line.
  - *word*—Specifies for the expression.
- **last [num]**—Displays the last lines to print. The optional *num* specifies the number of lines to print. The range is from 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
  - **|**—Pipe 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 modules installed in a Cisco router or switch. Data is logged to files that are 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.

This command does not require a license.

**Examples**

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

```
switch# show logging onboard module 2 boot-uptime
Sat Feb 29 18:11:38 2008: Boot Record
-----
Boot Time.....: Sat Feb 29 18:11:38 2008
Slot Number.....: 2
Serial Number....: JAB0912026U
Bios Version.....: v0.0.8(08/18/07)
Alt Bios Version...: v0.0.8(08/18/07)
Firmware Version...: 3.0(1) [build 3.0(0.291)]
switch#
```

Table 8 describes the significant fields shown in the display.

**Table 8** *show logging onboard boot-uptime Command Output*

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

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

```
switch# show logging onboard module 2 device-version
Device Version Records:
-----
Timestamp                Device Name           Instance  Hardware  Software
                          Num              Version    Version
-----
Sat Feb 29 18:11:38 2008 Stratosphere         0          1          1
Sat Feb 29 18:11:38 2008 Stratosphere         1          1          1
Sat Feb 29 18:11:38 2008 Skyline-asic          0          1          1
Sat Feb 29 18:11:38 2008 Tuscany-asic          0          1          0
Sat Feb 29 18:11:38 2008 X-Bus IO              0          6          0
Sat Feb 29 18:11:38 2008 Power Mngmnt Ep1     0          6          0
Sat Feb 29 18:42:01 2008 Stratosphere         0          1          1
Sat Feb 29 18:42:01 2008 Stratosphere         1          1          1
Sat Feb 29 18:42:01 2008 Skyline-asic          0          1          1
Sat Feb 29 18:42:01 2008 Tuscany-asic          0          1          0
Sat Feb 29 18:42:01 2008 X-Bus IO              0          6          0
Sat Feb 29 18:42:01 2008 Power Mngmnt Ep1     0          6          0
switch#
```

Table 9 describes the significant fields shown in the display.

**Table 9** *show logging onboard device-version Command Output*

Field	Description
Timestamp	Day, date, and time.
Device Name	Device name.

**Table 9** *show logging onboard device-version Command Output*

Field	Description
Instance Num	Number of instances.
Hardware Version	Hardware device version.
Software Version	Software device version.

This example shows how to display the OBFL exception log information:

```
switch# show logging onboard module 2 exception-log
Sun Feb 24 00:12:35 2008 : Exception Log Record
Device Id : 60
Device Name : DEV_SKYLINE_NI
Device Error Code : f(H)
Device Error Name : SKY_NI_ERR_BM_B1_3_BIST_FAILED
Sys Error : Skyline ni module experienced an error
Errtype : NON-CATASTROPHIC
PhyPortLayer : Fibre Channel
Port(s) Affected : 13-18
Error Description : Skyline BM B1_3 BIST for interface 2 timed out during init
DSAP : 0
UUID : 0
Time : Sun Feb 24 00:11:25 2008
switch#
```

[Table 10](#) describes the significant fields shown in the display.

**Table 10** *show logging onboard exception-log Command Output*

Field	Description
Sun Feb 24 00:12:35 2008:	Date and time the exception was recorded.
Device Id:	Device identification number.
Device Name:	Device name.
Device Error Code	Device specific error code.
Device Error Name:	Name of the device error.
Sys Error:	System error message.
Errtype:	Error type.
PhyPortLayer:	Physical layer type.
Port(s) Affected:	Number of the ports affected.
Error Description:	Description of the error.
DSAP:	Destination session announcement protocol (DSAP) identification.
UUID:	Universal unique identifier (UUID).

This example shows how to display the OBFL history information:

```
switch# show logging onboard module 2 obfl-history
OBFL history records:
-----
Sat Feb 29 30 18:09:57 2008 : OBFL all logs cleared
Sat Feb 29 18:47:53 2008 : OBFL miscellaneous-error logs cleared
```



```
Sat Feb 29 20:07:45 2008 : OBFL miscellaneous-error logs cleared
switch#
```

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

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

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

```
switch# show logging onboard module 2 stack-trace
===== STACK TRACE =====
Logging time: Sat Feb 29 19:47:38 2008
watchdog timeout: process swapper (0), jiffies 0x169bb
Stack: c0006e98 c001721c d195f5b4 c0005424 c0005500 c0003e90 c0005a2c c0005a40
c0001a88 c01bf610 c0000394
Call Trace:
print_stack2_buf + 0x50
kernel_thread + 0xb94
klm_cctrl + 0x4554
ppc_irq_dispatch_handler + 0x190
do_IRQ + 0x3c
ret_from_intercept + 0x0
probe_irq_mask + 0x494
probe_irq_mask + 0x4a8
transfer_to_handler + 0x15c
softnet_data + 0x2b0
Registers:
NIP: C0005A20 XER: 00000000 LR: C0005A2C SP: C01AA120 REGS: c01aa070 TRAP: 0500
Tainted: PF
MSR: 00009000 EE: 1 PR: 0 FP: 0 ME: 1 IR/DR: 00
DEAR: C0029B40, ESR: C01F0000
MCSRR0: 00000000, MCSRR1: 00000000, MCAR: 00000000
MCSR: 00000000 MCAR: 00000000 MCPSUMR: 00000000
TASK = c01a8190[0] 'swapper' Last syscall: 120
last math 00000000 last altivec 00000000 last spe 00000000
GPR00: 00000000 C01AA120 C01A8190 00000000 00000032 C8F1DE28 D1010A9F 00000000
GPR08: 0000180F C01FA39C D1010AA3 C01B8D18 24044244 1003A44C 0FFF6700 10049000
GPR16: 0FFAE1B0 0FFFAC90 00000000 00000000 00000000 00000000 00000001
GPR24: 00000000 00000000 00001160 007FFEAB 007FFE00 C01F0000 C01F0000 00000000
```

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.

This example shows how to display the OBFL error statistics:

```
switch# show logging onboard module 2 error-stats
-----
OBFL Data for
  Module: 2
-----
```

## show logging onboard

```
ERROR STATISTICS INFORMATION FOR DEVICE ID 80 DEVICE Eureka
```

```
-----
Error Stat Counter Name      |      Count      |      Time Stamp      |In|Port
                             |                 |MM/DD/YY HH:MM:SS   |st|Rang
                             |                 |                     |Id|e
-----
PB2_TX FlwCtrl from conn. ASIC > pe|0x1              |02/04/08 17:07:28|00|
riod Intr                    |                 |                   |||
PB2_TX FlwCtrl from conn. ASIC > pe|0x1              |02/06/08 10:54:44|00|
riod Intr                    |                 |                   |||
-----
```

```
ERROR STATISTICS INFORMATION FOR DEVICE ID 81 DEVICE Lamira
```

```
-----
Error Stat Counter Name      |      Count      |      Time Stamp      |In|Port
                             |                 |MM/DD/YY HH:MM:SS   |st|Rang
                             |                 |                     |Id|e
-----
NF2 Interrupt - NH HIT error  |0x1              |02/06/08 10:54:44|00|
-----
```

```
switch#
```

Table 11 describes the significant fields shown in the display.

**Table 11** show logging onboard error-stats Command Output

Field	Description
Error Stat Counter Name	Name of the error statistics counter.
Count	Total interrupt count.
Time Stamp MM/DD/YY HH:MM:SS	Time and date of the error.
Inst Id	Instance number.
Port The range is from	Range of ports affected.

The following example shows how to display the OBFL RxWait information:

```
switch# show logging onboard rxwait
```

```
-----
Module: 2 rxwait count
-----

Show Clock
-----
2017-10-05 11:42:22
Notes:
  - Sampling period is 20 seconds
  - Only rxwait delta >= 100 ms are logged

-----
| Interface      | Delta RxWait Time | Congestion | Timestamp |
|               | 2.5us ticks | seconds |           |
-----
| Eth2/11(VL3)  | 2880818 | 7 | 36% | Thu Sep 21 18:31:58 2017 |
| Eth2/30(VL3)  | 42200 | 0 | 0% | Thu Sep 14 15:05:15 2017 |
| Eth2/31(VL3)  | 40261 | 0 | 0% | Thu Sep 14 15:01:14 2017 |
| Eth2/29(VL3)  | 41155 | 0 | 0% | Thu Sep 14 14:47:54 2017 |
| Eth2/30(VL3)  | 40499 | 0 | 0% | Thu Sep 14 14:47:54 2017 |
-----
```

The following example shows how to display the OBFL Txwait information:

```
switch# show logging onboard txwait
```

```
-----
Module: 10 txwait count
-----

-----
Show Clock
-----
2017-08-28 17:01:30
```

```
Notes:
- Sampling period is 20 seconds
- Only txwait delta >= 100 ms are logged
```

```
-----
| Interface          | Delta TxWait Time      | Congestion | Timestamp
| 2.5us ticks | seconds |
-----
| Eth10/20 VL3)    | 882527 | 2 | 11% | Mon Aug 28 16:15:45 2017|
| Eth10/20 VL3)    | 5457256 | 13 | 68% | Mon Aug 28 16:15:24 2017|
-----
```

**Related Commands**

---

<b>clear logging onboard</b>	Clears the OBFL entries in the persistent log.
<b>hw-module logging onboard</b>	Enables or disabled OBFL entries based on the error type.

---

# 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.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

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

```
switch# show logging server
switch#
```

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

# 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.

---

**Defaults** None

---

**Command Modes** Any command mode

---

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

---

---

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

---

**Examples** This example shows how to display the logging session status:

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

# 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.

---

**Defaults** None

---

**Command Modes** Any command mode

---

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

---

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

---



---

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

---

**Examples** This example shows how to display the logging status:

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

# show logging timestamp

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

## **show logging timestamp**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the logging time stamp configuration:

```
switch# show logging timestamp
switch#
```

Related Commands	Command	Description
	<b>logging timestamp</b>	Configures the logging time stamp granularity.

# show maintenance snapshot-delay

To display the after\_maintenance snapshot-delay timer value, use the **show maintenance snapshot-delay** command.

**show maintenance snapshot-delay**

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

**Defaults** None

**Command Modes** Privileged EXEC

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	8.0(1)	This command was introduced.

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

**Examples** This example shows how to display the after\_maintenance snapshot-delay timer value:

```
switch# show maintenance snapshot-delay
after_maintenance snapshot delay value: 5000
```

Related Commands	Command	Description
	<b>system mode maintenance snapshot-delay delay-in-seconds</b>	Changes the snapshot-delay timer value. The default snapshot-delay timer value is 120 seconds.



# show module

To display module information, use the **show module** command.

```
show module [slot {bandwidth-fairness} | fabric [fabric-slot] | internal | uptime | xbar
            [xbar-slot]]
```

Syntax Description	
<i>slot</i>	(Optional) Number of the slot for an I/O module or a supervisor module.
<b>bandwidth-fairness</b>	Displays the status of the bandwidth fairness for the module.
<b>fabric</b>	(Optional) Displays the fabric information.
<i>fabric-slot</i>	(Optional) Number of slots for the fabric module.
<b>internal</b>	(Optional) Displays the line card manager related information.
<b>uptime</b>	(Optional) Displays the amount of time since the modules were reloaded.
<b>xbar</b>	(Optional) Displays information about a fabric module.
<i>xbar-slot</i>	(Optional) Number of the slot for the xbar module.

**Defaults** Displays module information for all I/O modules and supervisor modules in the chassis.

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.1(2)	Output modified to show diagnostic events.
	6.2(2)	Removed the <b>recovery-steps</b> keyword.

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

**Examples**

This example shows how to display information for all modules in the chassis:

```
switch# show module
Mod  Ports  Module-Type                Model                Status
---  ---
7    48     1000 Mbps Optical Ethernet Modul N7K-M148GS-11      ok
9    0      Supervisor module-1X          N7K-SUP1            active *
12   0      10/100/1000 Mbps Ethernet Module powered-dn

Mod  Power-Status  Reason
---  ---
12   powered-dn   Configured Power down

Mod  Sw          Hw
---  ---
7    4.1(3)     0.202
9    4.1(3)     0.805

Mod  MAC-Address(es)                Serial-Num
---  ---
7    00-1b-54-c2-ed-d0 to 00-1b-54-c2-ee-04 JAF1219AGFE
9    00-1b-54-c0-ff-10 to 00-1b-54-c0-ff-18 JAB114000BV

Mod  Online Diag Status
---  ---
7    Pass
9    Pass

Xbar Ports  Module-Type                Model                Status
---  ---
1    0      Fabric Module 1           N7K-C7018-FAB-1    ok

Xbar Sw          Hw
---  ---
1    NA          0.101

Xbar MAC-Address(es)                Serial-Num
---  ---
1    NA          JAF1225AGHJ

* this terminal session
switch#
```

This example shows how to display information for a specific module:

```
switch# show module 7
Mod  Ports  Module-Type                Model                Status
---  ---  ---
7    48    1000 Mbps Optical Ethernet Modul N7K-M148GS-11      ok

Mod  Sw                Hw
---  ---
7    4.1(3)            0.202

Mod  MAC-Address(es)                Serial-Num
---  ---
7    00-1b-54-c2-ed-d0 to 00-1b-54-c2-ee-04 JAF1219AGFE

Mod  Online Diag Status
---  ---
7    Pass

Chassis Ejector Support: Enabled
Ejector Status:
Left ejector CLOSE, Right ejector CLOSE, Module HW does not support ejector based shutdown.
switch#
```

This example shows how to display information for the fabric modules:

```
switch# show module xbar
Xbar Ports  Module-Type                Model                Status
---  ---  ---
1    0    Fabric Module 1            N7K-C7018-FAB-1    ok

Xbar Sw                Hw
---  ---
1    NA                0.101

Xbar MAC-Address(es)                Serial-Num
---  ---
1    NA                JAF1225AGHJ

* this terminal session
switch#
```

**Related Commands**

Command	Description
<b>show hardware</b>	Displays information about the hardware.
<b>show inventory</b>	Displays hardware inventory information.
<b>show diagnostic events</b>	Displays diagnostic events by error and information event type.

# show monitor

To display information about the Ethernet Switched Port Analyzer (SPAN), use the **show monitor** command.

## show monitor

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display information about a SPAN:

```
switch(config)# show monitor
Session State Reason Description
-----
1 down Session admin shut
6 down Session admin shut
8 down Session admin shut
9 down Session admin shut
switch(config)#
```

Related Commands	Command	Description
	<b>show running-config monitor</b>	Displays the running configuration to the startup configuration.
	<b>show startup-config monitor</b>	Displays information about the startup SPAN configuration.

# show monitor session

To display information about an Ethernet Switched Port Analyzer (SPAN) or a Encapsulated Remote Switched Port Analyzer (ERSPAN) session for analyzing traffic between ports, use the **show monitor session** command.

**show monitor session** { **all** | *session\_number* | **range** *session\_range* } [**brief**]

Syntax Description	all	Displays information about all SPAN or ERSPAN sessions.
	<i>session_number</i>	Specified SPAN or ERSPAN session number.
	<b>range</b> <i>session_range</i>	Displays information about the specified range of SPAN or ERSPAN sessions.
	<b>brief</b>	(Optional) Displays a brief summary of the information for the specified SPAN or ERSPAN session.

**Defaults** Displays a brief summary of information for all configured SPAN or ERSPAN sessions.

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

Command History	Release	Modification
	6.1(1)	Changed the command output for ERSPAN-source sessions.
	4.0(1)	This command was introduced.

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

**Examples** This example shows how to display information for all configured ERSPAN sessions:

```
switch(config)# show monitor session 2
  session 2
-----
type           : erspan-source
state          : up
erspan-id      : 100
vrf-name       : default
acl-name       : acl-name not specified
ip-ttl         : 255
ip-dscp        : 0
destination-ip : 10.1.1.2
```

## show monitor session

```

origin-ip      : 3.3.3.3 (global)
source intf   :
    rx        : Eth7/15
    tx        : Eth7/15
    both      : Eth7/15
source VLANs  :
    rx        :
    tx        :
    both      :
filter VLANs  : filter not specified

```

Feature	Enabled	Value	Modules Supported	Modules Not-Supported
Rate-limiter	No			
MTU-Trunc	No			
Sampling	No			
MCBE	No			
L3-TX	-	-	2 4 5 7	3 10
ERSPAN-ACL	-	-	4 7	2 3 5 10

Legend:

MCBE = multicast best effort  
L3-TX = L3 Multicast Egress SPAN

```

switch(config-erspan-src)# show monitor session 2
    session 2

```

```

-----
type           : erspan-source
version        : 3
state          : up
erspan-id      : 100
granularity    : 100 microseconds
vrf-name       : default
acl-name       : acl-name not specified
ip-ttl         : 255
ip-dscp        : 0
destination-ip : 10.1.1.2
origin-ip      : 3.3.3.3 (global)
source intf    :
    rx         : Eth7/15
    tx         : Eth7/15
    both       : Eth7/15
source VLANs  :
    rx         :
    tx         :
    both       :
filter VLANs  : filter not specified

```

Feature	Enabled	Value	Modules Supported	Modules Not-Supported
Rate-limiter	No			
MTU-Trunc	No			
Sampling	No			
MCBE	No			
L3-TX	-	-	2 4 5 7	3 10
ERSPAN-ACL	-	-	4 7	2 3 5 10
ERSPAN-V3	Yes	-	2 3 4 10	5 7

Legend:

MCBE = multicast best effort

L3-TX = L3 Multicast Egress SPAN

**Related Commands**

Command	Description
<b>monitor session</b>	Places you into monitor configuration mode for configuring a SPAN or ERSPAN session.

# 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** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	5.0(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(config)# show ntp access-groups
-----
Access List                               Type
-----
Admin_Group_123                           Peer
switch(config)#
```

Related Commands	Command	Description
	<b>ntp access-group peer</b>	Configures an NTP access group.



# 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** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	5.0(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(config)# show ntp authentication-keys
-----
Auth key          MD5 String
-----
3                 cisco
42                Nice_Key
34567             nexus7k
switch(config)#
```

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

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** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	5.0(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:

```
switch(config)# show ntp authentication-status
Authentication enabled.
switch(config)#
```

Related Commands	Command	Description
	<b>ntp authenticate</b>	Enables NTP authentication.
	<b>show ntp authentication-keys</b>	Displays the configured NTP authentication keys.

# show ntp internal

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

```
show ntp internal { event-history [config | fsm | msgs | rts | tstamp] | mem-stats [detail] |
module-info }
```

Syntax Description		
<b>event-history</b>		Specifies the event history.
<b>config</b>	(Optional)	Specifies the configuration history.
<b>fsm</b>	(Optional)	Specifies the finite state machine (FSM) state transition.
<b>msgs</b>	(Optional)	Specifies the message and transaction service (MTS) message history.
<b>rts</b>	(Optional)	Specifies the request-to-send (RTS) history.
<b>tstamp</b>	(Optional)	Specifies the timestamp update history.
<b>mem-stats</b>		Specifies memory allocation statistics of NTP.
<b>detail</b>	(Optional)	Specifies the memory allocation statistics of NTP in detail.
<b>module-info</b>		Specifies all line card-related information.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples**

This example shows how to display the NTP internal information:

```
switch(config)# show ntp internal module-info
Number of Linecards present = 4
Timestamp check (configured) = enabled
Timestamp check status = disabled
Enable/Disable status
-----
User : not disabled
SUP : not disabled
Fabric : not disabled
switch(config)#
```

**Related Commands**

Command	Description
<b>show running-config ntp</b>	Displays the NTP information.
<b>show ntp statistics</b>	Displays the NTP statistics.

# 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** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	5.0(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(config)# show ntp logging-status
NTP logging enabled.
switch(config)#
```

Related Commands	Command	Description
	<b>ntp logging</b>	Enables NTP logging.
	<b>show ntp authentication-status</b>	Displays the status of NTP authentication.
	<b>show ntp session status</b>	Displays the NTP CFS distribution session information.

# show ntp peers

To display the configured Network Time Protocol (NTP) servers and peers, use the **show ntp peers** command.

**show ntp peers**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

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

**Usage Guidelines** A domain name is resolved only when you have a domain name server (DNS) server configured. This command does not require a license.

**Examples** This example shows how to display all the configured NTP servers and peers:

```
switch(config)# show ntp peers
-----
Peer IP Address          Serv/Peer
-----
2001:db8::4101          Peer (configured)
192.0.2.10               Server (configured)
switch(config)#
```

Related Commands	Command	Description
	<b>ntp server</b>	Configures an NTP server.
	<b>ntp peer</b>	Configures an NTP peer.
	<b>show ntp peer-status</b>	Displays the status of all the server and peers.

# show ntp peer-status

To do 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.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the peer status for NTP:

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

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

# 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** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(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
	<b>show ntp source</b>	Displays information about the NTP source.
	<b>show ntp peers</b>	Displays information about NTP peers.



# 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** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(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
	<b>show ntp source</b>	Displays information about the NTP source.
	<b>show ntp peers</b>	Displays information about NTP peers.

# 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

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(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
	<b>show ntp source</b>	Displays information about the NTP source.
	<b>show ntp peers</b>	Displays information about NTP peers.

# 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

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(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
	<b>show ntp source</b>	Displays information about the NTP source.
	<b>show ntp peers</b>	Displays information about NTP peers.

# show ntp rts-update

To display if the request to send (RTS) update is enabled, use the **show ntp rts-update** command.

## show ntp rts-update

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to view RTS-update information:

```
switch(config)# show ntp rts-update
RTS update is enabled
switch(config)#
```

Related Commands	Command	Description
	<b>show ntp source-interface</b>	Displays information about the NTP source.

# 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

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.0(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:  
switch(config)# **show ntp source**

Related Commands	Command	Description
	<b>ntp source</b>	Configures the NTP source.

# 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

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(3)	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
	<b>show startup-config ntp</b>	Displays information about the startup NTP configuration of the switch.
	<b>show running-config ntp</b>	Displays information about the NTP configuration that is currently running on the switch.

# 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		
<b>io</b>		Displays the input-output statistics.
<b>local</b>		Displays the counters maintained by the local NTP.
<b>memory</b>		Displays the statistics counters related to the memory code.
<b>peer</b>		Displays the per-peer statistics counter of a peer.
<b>ipaddr address</b>		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 hex A:B::C:D.
<b>name name</b>		Displays statistics for one or more named peers.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to displays statistics for NTP:

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

Related Commands	Command	Description
	<b>clear ntp statistics</b>	Clears NTP statistics.

# show ntp status

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

```
show ntp status [ > | >> | | ]
```

Syntax Description	
>	(Optional) Redirects the command output to a file.
>>	(Optional) Redirects the command output to a file in append mode.
	(Optional) Pipes the command output to a filter.

**Defaults** Disabled

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

**Usage Guidelines** This command shows whether Cisco Fabric Services (CFS) is enabled or disabled for the NTP application and whether a fabric lock is in place because a configuration is in progress.

This command does not require a license.

**Examples** This example shows how to display the CFS distribution status for NTP. In this example, CFS distribution is enabled and the fabric is locked. When a configuration is in progress on a CFS-enabled device, the fabric is locked until the change is committed and the configuration is distributed throughout the fabric. The lock prevents multiple configurations occurring at the same time.

```
switch(config)# show ntp status
Distribution : Enabled
Last operational state: Fabric Locked
```



**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show cfs status</b>	Displays the global CFS distribution status (enabled/disabled) for the device.
<b>clear ntp session</b>	Clears the application configuration session, discards pending changes, and releases the lock on the fabric.
<b>ntp distribute</b>	Enables the device to receive NTP configuration updates distributed through CFS.
<b>cfs distribute</b>	Globally enables CFS distribution for all applications on the device, including CFS over IP.
<b>ntp enable</b>	Enables NTP on a device. NTP is enabled by default.

# 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

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

Command History	Release	Modification
	5.0(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)#
```

Related Commands	Command	Description
	<b>ntp trusted-keys</b>	Displays the configured NTP authentication keys.

# show platform hardware capacity interface resources

To display a summary of current platform hardware resource utilization, use the **show platform hardware capacity interface resources** command.

**show platform hardware capacity interface resources**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to display a summary of current platform hardware resource utilization:

```
switch# show platform hardware capacity interface resources
Interface Resources

Interface drops:
  Module      Total drops:  Tx              Rx  Highest drop port: Tx Rx
              7              0              0              -  -

Interface buffer sizes:
  Module      Bytes:  Tx buffer      Rx buffer
              7              6452775        7743330
```

Related Commands	Command	Description
	<b>show hardware fabric-utilization</b>	Display information about fabric utilization.

# show port-monitor

To display information about the Simple Network Management Protocol (SNMP) port-monitor configuration, use the **show port-monitor** command.

**show port-monitor** [*policy-name*]

<b>Syntax Description</b>	<i>policy-name</i> (Optional) Policy name. The maximum number of alphanumeric characters is 32.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.1(2)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display the SNMP port-monitor information:
-----------------	--

```
switch(config)# show port-monitor name pm2
switch(config-port-monitor)# show port-monitor pm2
```

```
Policy Name : pm2
Admin status : Not Active
Oper status : Not Active
Port type : All Ports
```

```
-----
Counter      Threshold  Interval  Rising  Threshold  event  Falling  Threshold  event  In
Use
-----  -----  -----  -----  -----  -----  -----  -----  -----  -
-----
Link Loss    Delta      60        5        4          1          4
  Yes
Sync Loss    Delta      60        5        4          1          4
  Yes
Protocol Error  Delta      60        1        4          0          4
  Yes
Signal Loss    Delta      60        5        4          1          4
```

```

      Yes
Invalid Words   Delta    60    1    4    0    4
      Yes
Invalid CRC's   Delta    60    5    4    1    4
      Yes
RX Performance  Delta    60    2147483648    4    524288000    4
      Yes
TX Performance  Delta    60    2147483648    4    524288000    4
      Yes
-----
switch(config-port-monitor)#
    
```

**Related Commands**

Command	Description
<b>show port-monitor status</b>	Displays the port-monitor status.
<b>show port-monitor active</b>	Displays active port-monitor policies.

# show port-monitor active

To display information about the active Simple Network Management Protocol (SNMP) port-monitor policies, use the **show port-monitor active** command.

## show port-monitor active

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to display information about the active SNMP port-monitor policies:

```
switch(config)# show port-monitor active
```

```
Policy Name : test
Admin status : Active
Oper status : Active
Port type : All Ports
```

```
-----
Counter      Threshold  Interval  Rising  Threshold  event  Falling  Threshold  e
vent In Use
-----  -----  -----  -----  -----  -----  -----  -----
Link Loss    Delta      60        5        4          1        4
  Yes
Sync Loss    Delta      60        5        4          1        4
  Yes
Protocol Error  Delta      60        1        4          0        4
  Yes
Signal Loss    Delta      60        5        4          1        4
  Yes
Invalid Words  Delta      60        1        4          0        4
```

```

      Yes
Invalid CRC's   Absolute   30      10000000      100   1           4
      Yes
RX Performance   Delta     60      2147483648     4     524288000   4
      Yes
TX Performance   Delta     60      2147483648     4     524288000   4
      Yes
-----
-----
switch(config)#
    
```

**Related Commands**

Command	Description
<b>show port-monitor status</b>	Displays the port-monitor status.
<b>show port-monitor active</b>	Displays active port-monitor policies.

# show port-monitor status

To display information about the Simple Network Management Protocol (SNMP) port-monitor status, use the **show port-monitor status** command.

**show port-monitor status**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to display the SNMP port-monitor status:

```
switch(config)# show port-monitor status
Port Monitor      : Enabled
Active Policies   : None

Last 10 logs :

switch(config-port-monitor)#
```

Related Commands	Command	Description
	<b>show port-monitor active</b>	Displays active port-monitor policies.
	<b>show port-monitor</b>	Displays information about the port-monitor configuration.



# show processes

To display the process information for a device, use the **show processes** command.

```
show processes [vdc vdc-number]
```

<b>Syntax Description</b>	<b>vdc vdc-number</b> (Optional) Displays process information for a specific virtual device context (VDC).
---------------------------	--

**Defaults** Displays information for all processes in the local device.

**Command Modes** Any command mode

**Supported User Roles** network-admin  
vdc-admin  
network-operator  
vdc-operator

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

**Usage Guidelines** You can specify another VDC only from the default VDC.  
This command does not require a license.

**Examples** This example shows how to display the process information for a device:

```
switch# show processes
```

PID	State	PC	Start_cnt	TTY	Type	Process
1	S	b7f9e468	1	-	O	init
2	S	0	1	-	O	migration/0
3	S	0	1	-	O	ksoftirqd/0
4	S	0	1	-	O	desched/0
5	S	0	1	-	O	migration/1
6	S	0	1	-	O	ksoftirqd/1
7	S	0	1	-	O	desched/1
8	S	0	1	-	O	events/0
9	S	0	1	-	O	events/1
10	S	0	1	-	O	khelper
15	S	0	1	-	O	kthread
...						

This example shows how to display the process information for another VDC:

```
switch# show processes vdc 2
```

PID	State	PC	Start_cnt	TTY	Type	Process
1	S	b7f9e468	1	-	O	init
2	S	0	1	-	O	migration/0
3	S	0	1	-	O	ksoftirqd/0
4	S	0	1	-	O	desched/0
5	S	0	1	-	O	migration/1
6	S	0	1	-	O	ksoftirqd/1
7	S	0	1	-	O	desched/1
8	S	0	1	-	O	events/0
9	S	0	1	-	O	events/1
10	S	0	1	-	O	khelper
15	S	0	1	-	O	kthread
...						

# show processes cpu

To display the CPU utilization information for processes on the device, use the **show processes cpu** command.

## show processes cpu

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

**Defaults** Displays information for all processes in the local device.

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

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

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

**Examples** This example shows how to display the CPU utilization information for the processes:

```
switch# show processes cpu
```

PID	Runtime (ms)	Invoked	uSecs	1Sec	Process
1	286	315748	0	0	init
2	302	636268	0	0	migration/0
3	1586	72636726	0	0	ksoftirqd/0
4	502	1345165	0	0	desched/0
5	1956	559740	3	0	migration/1
6	2218	457761883	0	0	ksoftirqd/1
7	2325	1469647	1	0	desched/1
8	1158	794795	1	0	events/0
9	1258	721210	1	0	events/1
10	62	2779	22	0	khelper
15	0	30	25	0	kthread
24	0	2	5	0	kacpid
102	201	286	704	0	kblockd/0
103	276	516	535	0	kblockd/1
116	0	5	17	0	khubd
...					

# show processes cpu history

To display information about the CPU utilization by the system processes in the last 60 seconds, 60 minutes, and 72 hours in a graphical format, use the **show processes cpu history** command.

## show processes cpu history

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

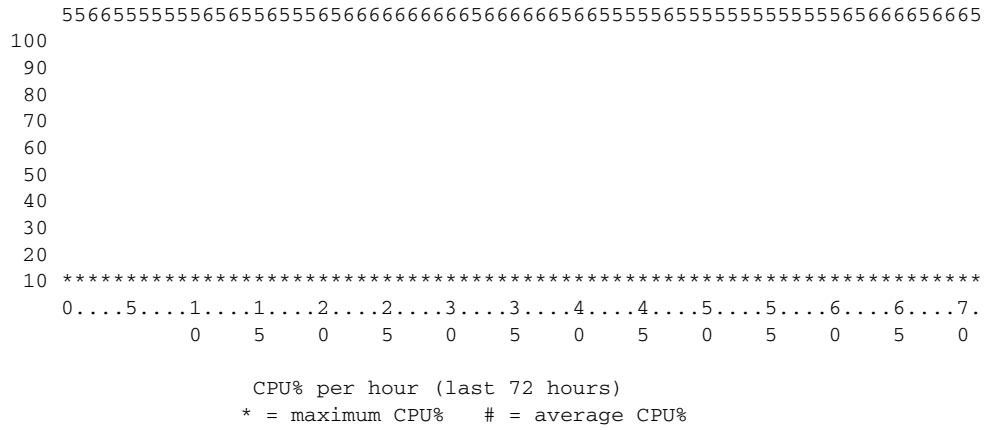
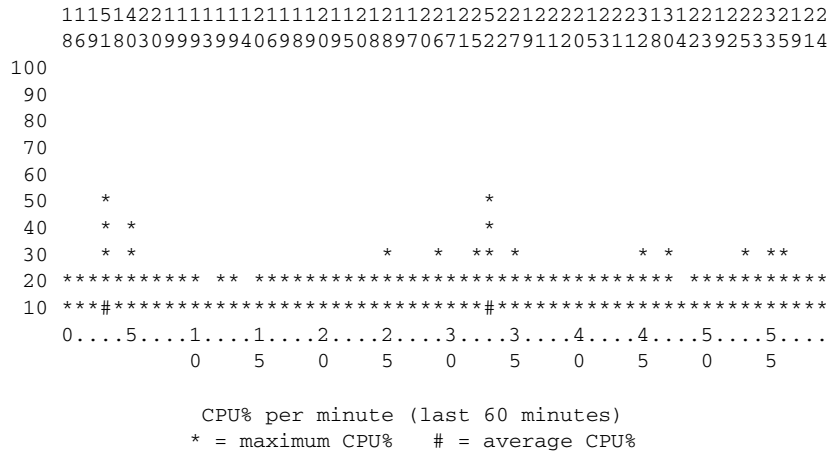
**Usage Guidelines** This command does not require a license.

**Examples** This example shows how to display information about the CPU utilization by the system processes for last 60 seconds, 60 minutes, and 72 hours in a graphical format:

```
switch(config)# show processes cpu history

92      5  4   73   474      64   65 575   47
      206324551543534226644368135103343343133313901236334538431915
100
90 #
80 #           #
70 #           #           #           #           #
60 #           #           #           #           #           #
50 #           # #           #           #           #           #
40 #           # #           #           #           #           #
30 #           # #           #           #           #           #
20 ##          # #           #           #           #           #
10 ###         # # #         #           #           #           # # # # #
      0...5...1...1...2...2...3...3...4...4...5...5...
      0      5      0      5      0      5      0      5      0      5

      CPU% per second (last 60 seconds)
      # = average CPU%
```



**Related Commands**

Command	Description
show processes cpu	Displays the CPU utilization information for processes on the device.
show system resources	Displays the system resources.

# show process cpu sort

To display information about CPU processes sorted by CPU utilization, use the **show process cpu sort** command.

**show process cpu sort [5sec | 1min | 5min]**

Syntax Description		
<b>5sec</b>	(Optional)	Displays the sorted output based on the processes that use the memory for five seconds.
<b>1min</b>	(Optional)	Displays the sorted output based on the processes that use the memory for one minute.
<b>5min</b>	(Optional)	Displays the sorted output based on the processes that use the memory for five minutes.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	6.2(2)	Added the <b>5sec</b> , <b>1min</b> , and <b>5min</b> keywords.
	4.1(1)	This command was introduced.

**Usage Guidelines**

The modules perform the polling and send messages to the supervisor module for Simple Network Management Protocol (SNMP) caching. When attached to a module under no load, the CPU spikes approximately every 10 seconds for a short period of time. The name of the process is statsclient.

The CPU spike can go up to 100 percent for a few milliseconds. The process is preemptive and it does not block other high priority processes.

This command does not require a license.

**Examples** This example shows how to display information about CPU processes sorted by CPU utilization:

```
switch(config)# show process cpu sort
```

```

PID      Runtime(ms)   Invoked    uSecs   1Sec   Process
-----
3622      2335          6843      341     50.0%  pfstat

```

```

 1      2550      4169      611      0.0%  init
 2         13       2676         4      0.0%  migration/0
 3      2091     883525         2      0.0%  ksoftirqd/0
 4         48       6300         7      0.0%  desched/0
 5         10       2816         3      0.0%  migration/1
 6         21    4450597         0      0.0%  ksoftirqd/1
 7         42       6416         6      0.0%  desched/1
 8      1785      8581      208      0.0%  events/0
 9      1560      7426      210      0.0%  events/1
10         58      2731         21      0.0%  khelper
15         0         30         25      0.0%  kthread
24         0         2          5      0.0%  kacpid
104        12         201         62      0.0%  kblockd/0
105         4         138         33      0.0%  kblockd/1
118         0         5         17      0.0%  khubd
185         0         4          3      0.0%  pdflush
186        139      3010         46      0.0%  pdflush
187         0         1          5      0.0%  kswapd0
--More--

```

**Note**

Because the values in the 1Sec column represent a dual-core CPU, the CPU processes may add up to 200 percent. In this example, the pfstat process is consuming 50 percent of one core.

**Related Commands**

Command	Description
<b>show processes cpu</b>	Displays the CPU utilization information for processes on the device.
<b>show processes cpu history</b>	Displays information about the CPU utilization by the system processes in the last 60 seconds, 60 minutes, and 72 hours in a graphical format.

# show processes log

To display the contents of the process log, use the **show processes log** command.

**show processes log** [**details** | **pid** *process-id* | **vdc-all**]

Syntax Description	details	(Optional) Displays detailed information from the process log.
	<b>pid</b> <i>process-id</i>	(Optional) Displays detailed information from the process log for a specific process. The range is from 1 to 2147483647.
	<b>vdc-all</b>	(Optional) Displays process log information for all virtual device contexts (VDCs).

**Defaults** Displays summary information for all processes on the device.

**Command Modes** Any command mode

**Supported User Roles** network-admin  
vdc-admin  
network-operator  
vdc-operator

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

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

**Examples** This example shows how to display summary information from the process log:

```
switch# show processes log
VDC Process          PID      Normal-exit  Stack  Core  Log-create-time
-----
 1 aclmgr             3632          N      Y      N  Thu Mar 13 21:37:07 2008
 1 aclmgr             4182          N      Y      N  Wed Mar 12 13:45:38 2008
 1 aclmgr             4205          N      Y      N  Wed Mar 12 13:45:38 2008
 1 adjmgr             4333          N      N      N  Sat Nov 24 06:25:20 2007
 1 arbiter            4332          N      Y      N  Mon Nov 19 10:14:42 2007
 1 arp                 3870          N      Y      N  Sat Dec 22 12:02:46 2007
 1 clis                10005         N      Y      N  Sat Nov 24 03:46:13 2007
 1 clis                10268         N      N      N  Fri Dec 14 09:13:53 2007
 1 clis                1040          N      Y      N  Fri Nov 16 13:34:30 2007
...
```



This example shows how to display detailed information from the process log:

```
switch# show processes log details
=====
Service: aclmgr
Description: ACL Mgr

Started at Thu Mar 13 20:34:35 2008 (507163 us)
Stopped at Thu Mar 13 20:37:07 2008 (664205 us)
Uptime: 2 minutes 32 seconds

Start type: SRV_OPTION_RESTART_STATELESS (23)
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2)
System image name: n7000-s1-dk9.4.0.1.gbin
System image version: 4.0(1) S7

PID: 3632
Exit code: signal 11 (core dumped)

CWD: /var/sysmgr/work

Virtual Memory:

CODE      08048000 - 0811CCF4
DATA      0811DCF4 - 0811EBE8
BRK       08121000 - 08259000
STACK     BFFFE270
TOTAL     47244 KB

Register Set:

EBX B7D64CD0      ECX 00000001      EDX 00000001
ESI 41170040      EDI 00000000      EBP BFFFD1C8
EAX 00000401      XDS C010007B      XES 0000007B
EAX FFFFFFFF (orig) EIP B7D5BEF2      XCS 00000073
EFL 00010292      ESP BFFFD1C0      XSS 0000007B

Stack: 4272 bytes. ESP BFFFD1C0, TOP BFFFE270

0xBFFFD1C0: B7D5BEE0 B7D64CD0 BFFFD1D8 B7D5C381 .....L.....
0xBFFFD1D0: B7D2614C FF000226 BFFFD218 B7D232BA La..&.....2..
0xBFFFD1E0: B5542014 B7D25DE0 000007DE B5542014 . T..]..... T.
0xBFFFD1F0: B7D08918 B7D2614C FF000226 08241A54 ....La..&...T.$
0xBFFFD200: B5542014 41170034 08241A54 B7D2614C . T.4..AT$.La..
0xBFFFD210: FF000226 BFFFD2D0 BFFFD278 B7D138CE &.....x....8..
0xBFFFD220: 08246A04 08230074 BFFFD2D0 B7D5A24D .j$.t.#.....M...
0xBFFFD230: B7D6369A 00002000 00000004 00000000 .6... ..
0xBFFFD240: 0000C005 00002000 BFFFD278 B7D3CF90 ..... ..x.....
...
```

This example shows how to display detailed information from the process log for a specific process:

```
switch# show processes pid 3632
=====
Service: arp
Description: Address Resolution Protocol (ARP)

Started at Sat Dec 22 12:02:19 2007 (216828 us)
Stopped at Sat Dec 22 12:02:44 2007 (496964 us)
Uptime: 25 seconds

Start type: SRV_OPTION_RESTART_STATELESS (23)
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2)
System image version: 4.0(0.788) S16

PID: 3912
Exit code: signal 11 (core dumped)

Threads: 3906 3905 4066 3917 3884 3870

CWD: /var/sysmgr/work

Virtual Memory:

      CODE      08048000 - 08071474
      DATA     08072474 - 08074794
      BRK       08075000 - 080DE000
      STACK     BFFFEB80
      TOTAL     107908 KB

Register Set:

      EBX B7EF4264      ECX B53F45CA      EDX B8009B1E
      ESI B601C003      EDI B53F45C8      EBP B53F4578
      EAX B8009B1E      XDS 0000007B      XES 0000007B
      EAX FFFFFFFF (orig) EIP B7EDF9AB      XCS 00000073
      EFL 00010286      ESP B53F4560      XSS 0000007B

Stack: 2688 bytes. ESP B53F4560, TOP BFFFEB80

0xB53F4560: B601C003 00000001 F1EC838D B7EF4264 .....dB..
0xB53F4570: 00000000 00000000 B53F45D8 B7EE0C0D .....E?.....
0xB53F4580: B601C003 B53F45CA B53F45C8 B53F45C0 .....E?..E?..E?.
0xB53F4590: 00000001 B53F45C4 00000000 00000001 .....E?.....
...
```

This example shows how to display process log information for all VDCs on the physical device:

```
switch# show processes log vdc-all
VDC Process          PID      Normal-exit  Stack  Core  Log-create-time
-----
1 aclmgr             3632      N           Y      N      Thu Mar 13 21:37:07 2008
1 aclmgr             4182      N           Y      N      Wed Mar 12 13:45:38 2008
1 aclmgr             4205      N           Y      N      Wed Mar 12 13:45:38 2008
1 adjmgr             4333      N           N      N      Sat Nov 24 06:25:20 2007
1 arbiter            4332      N           Y      N      Mon Nov 19 10:14:42 2007
1 arp                3870      N           Y      N      Sat Dec 22 12:02:46 2007
1 clis               10005     N           Y      N      Sat Nov 24 03:46:13 2007
1 clis               10268     N           N      N      Fri Dec 14 09:13:53 2007
1 clis               1040      N           Y      N      Fri Nov 16 13:34:30 2007
1 clis               10486     N           Y      N      Fri Nov 16 14:58:59 2007
1 clis               10646     N           Y      N      Fri Nov 16 14:59:45 2007
...
```

# show processes memory

To display the memory allocation information for processes, use the **show processes memory** command.

**show processes memory [shared | sort]**

Syntax Description	shared	(Optional) Displays the shared memory allocation.
	sort	(Optional) Displays the sorted list that is based on the memory usage.

**Defaults** Displays memory allocated to the processes.

**Command Modes** Any command mode

**Supported User Roles** network-admin  
vdc-admin  
network-operator  
vdc-operator

Command History	Release	Modification
	6.2(2)	Added the <b>sort</b> keyword.
	4.0(1)	This command was introduced.

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

**Examples** This example shows how to display information about memory allocation for processes:

```
switch# show processes memory
```

```

PID      MemAlloc  StackBase/Ptr  Process
-----
 1      147456    bffffda0/bffff890  init
 2           0           0/0             migration/0
 3           0           0/0             ksoftirqd/0
 4           0           0/0             desched/0
 5           0           0/0             migration/1
 6           0           0/0             ksoftirqd/1
 7           0           0/0             desched/1
 8           0           0/0             events/0
 9           0           0/0             events/1
10           0           0/0             khelper
15           0           0/0             kthread
24           0           0/0             kacpid
...

```

This example shows how to display information about shared memory allocation for processes:

```
switch# show processes memory shared
Component          Shared Memory      Size      Used  Available  Reference
                   Address      (kbytes)  (kbytes)  (kbytes)  Count
smm                0X60000000      1024         3       1021      115
cli                0X60110000     24576*      13991    10585     84
am                 0X61920000     14336*       14     14322      7
urib               0X62730000     32768*       648    32120     25
u6rib-ufdm        0X64740000       320*       188      132      2
urib-redis        0X647A0000     4096*        0     4096     25
icmpv6            0X64BB0000     2048         0       2048      2
ip                 0X64DC0000     8192         65     8127     23
urib-ufdm         0X655D0000     2048*        0     2048      2
u6rib             0X657E0000    16384*       507    15877     12
ipv6              0X667F0000     8192         2     8190      9
u6rib-notify      0X67000000     2048*       681    1367     12
rpm               0X67210000     2048         6     2042     11
mrrib             0X67420000    40960         2    40958      3
mrrib-mfdm        0X69C30000     5120         0     5120      2
m6rib            0X6A140000    10240         2    10238      3
m6rib-mfdm        0X6AB50000     2048         10     2038      2
igmp              0X6AD60000     8192         0     8192      2
bgp               0X6B570000     8192        182     8010      1
Shared memory totals - Size: 189 MB, Used: 16 MB, Available: 173 MB
Free Physical Memory: 0 MB kernel, 0 MB user
```

#### Related Commands

Command	Description
<b>show processes</b>	Displays process information.
<b>show startup-config</b>	Displays the startup configuration.

# show ptp brief

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.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	5.2(1)	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
-----
Eth7/10      Passive
Eth7/1       Slave
```

This example shows how to display a brief display of the status of the PTP interfaces. The output below indicates that multiple ports that can be in master, passive, disabled, or uncalibrated states but only one port can be in slave state:

```
switch# show ptp brief
PTP port status
-----
Port State
-----
Eth1/1 Master
Eth1/15 Slave
Eth1/31 Master
Eth1/32 Master
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ptp clock</b>	Displays the properties of the local clock.
	<b>show ptp clocks foreign-masters-record</b>	Displays the state of foreign masters known to the PTP process.
	<b>show ptp counters</b>	Displays PTP specific packet counters for all Ethernet interfaces or for a specified interface.
	<b>show ptp corrections</b>	Displays the last few PTP corrections.
	<b>show ptp delay</b>	Displays the link delay and residence delay status of the PTP interface.
	<b>show ptp parent</b>	Displays the properties of the PTP parent.
	<b>show ptp port</b>	Displays the status of the PTP port.
	<b>show ptp time-property</b>	Displays the properties of the PTP clock.

# 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.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	5.2(1)	This command was introduced.
	7.3(0)D1(1)	This command was modified. The field <i>PTP Device Type</i> has been removed from the output. The fields <i>PTP Device Mode</i> , <i>PTP Device Encapsulation</i> , <i>PTP SwitchLatency Estimated</i> have been added to the output.
	7.3(0)DX(1)	This command was modified. The fields <i>PTP Source IP Address</i> , <i>Two-Step Clock Mode</i> , and <i>Slave-Only Clock Mode</i> have been added to the output.

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

**Examples** This example shows how to display the PTP clock information. The below output indicate that the PTP device is running in gPTP mode. The field description is self-explanatory.

```
switch# show ptp clock

PTP Device Mode : boundary-clock
PTP Device Encapsulation : layer-3
PTP Source IP Address : 1.1.1.1
PTP SwitchLatency Estimated : 5000(ns)
Clock Identity : 84:78:ac:ff:fe:56:bc:c1
Clock Domain : 0
Two-Step Clock Mode : Enabled
Slave-Only Clock Mode : Disabled
Number of PTP ports : 1
Priority1 : 255
Priority2 : 255
Clock Quality :
```

## ■ show ptp clock

```

Class : 248
Accuracy : 254
Offset (log variance) : 65535
Offset From Master : 0
Mean Path Delay : 0
Steps removed : 0
Local clock time : Tue Mar 15 02:23:45 2016

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ptp brief</b>	Displays the PTP status.
<b>show ptp clocks foreign-masters-record</b>	Displays the state of foreign masters known to the PTP process.
<b>show ptp counters</b>	Displays PTP specific packet counters for all Ethernet interfaces or for a specified interface.
<b>show ptp corrections</b>	Displays the last few PTP corrections.
<b>show ptp delay</b>	Displays the link delay and residence delay status of the PTP interface.
<b>show ptp parent</b>	Displays the properties of the PTP parent.
<b>show ptp port</b>	Displays the status of the PTP port.
<b>show ptp time-property</b>	Displays the properties of the PTP clock.



# 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 clocks foreign-masters-record** command.

```
show ptp clock foreign-masters-record {interface [ethernet slot/port]}
```

## Syntax Description

<b>interface</b>	Specifies an interface.
<b>ethernet slot/port</b>	(Optional) Specifies an Ethernet interface.

## Defaults

None

## Command Modes

Any command mode

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
5.2(1)	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. The below output indicates that the Ethernet 1/15 is receiving Announce messages correctly.

```
switch# show ptp clocks foreign-masters-record interface Ethernet 1/1
```

```
P1=Priority1, P2=Priority2, C=Class, A=Accuracy,
```

```
OSLV=Offset-Scaled-Log-Variance, SR=Steps-Removed
```

```
GM=Is grandmaster
```

```
-----  
Interface Clock-ID P1 P2 C A OSLV SR
```

```
-----  
Eth1/15 22:22:22:ff:fe:22:22:22 128 248 6 35 0 0 GM
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ptp brief</b>	Displays the PTP status.
	<b>show ptp clock</b>	Displays the properties of the local clock.
	<b>show ptp counters</b>	Displays PTP specific packet counters for all Ethernet interfaces or for a specified interface.
	<b>show ptp corrections</b>	Displays the last few PTP corrections.
	<b>show ptp parent</b>	Displays the properties of the PTP parent.
	<b>show ptp port</b>	Displays the status of the PTP port.
	<b>show ptp time-property</b>	Displays the properties of the PTP clock.

# 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.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	5.2(1)	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:

```
switch# show ptp corrections
PTP corrections
-----
Slave Port      Sup time        Corrections(s,ns)
-----
Eth7/10         2010 Mar 11 03:14:55  -1 1210900
Eth7/10         2010 Mar 11 03:14:55  -340978
```

Related Commands	Command	Description
	<b>show ptp brief</b>	Displays the PTP status.
	<b>show ptp clock</b>	Displays the properties of the local clock.
	<b>show ptp clocks foreign-masters-record</b>	Displays the state of foreign masters known to the PTP process.
	<b>show ptp counters</b>	Displays PTP specific packet counters for all Ethernet interfaces or for a specified interface.

<b>Command</b>	<b>Description</b>
<b>show ptp parent</b>	Displays the properties of the PTP parent.
<b>show ptp port</b>	Displays the status of the PTP port.
<b>show ptp time-property</b>	Displays the properties of the PTP clock.

# show ptp counters

To display the Precision Time Protocol (PTP) packet counters for all Ethernet interfaces or for a specified interface, use the **show ptp counters** command.

**show ptp counters** [**all** | **interface** *interface-name slot/port*]

<b>Syntax Description</b>	<i>interface-name</i> <i>slot/port</i>	Specifies an interface name and slot/port number.
---------------------------	---	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>Supported User Roles</b>	network-admin network-operator vdc-admin vdc-operator
-----------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.3(0)DX(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display the PTP counters of the Ethernet interface:

```
switch# show ptp counters interface ethernet 4/47
PTP Packet Counters of Interface Eth4/47:
-----
Packet Type                TX                RX
-----
Announce                    2                 294
Sync                        1                 147
FollowUp                    1                 147
Delay Request               113                0
Delay Response              0                 113
PDelay Request              0                  0
PDelay Response             0                  0
PDelay Followup             0                  0
Management                  0                  0
-----
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear ptp counters</b>	Clears PTP specific packet counters for all Ethernet interfaces or for a specified interface.
	<b>show ptp brief</b>	Displays the PTP status.
	<b>show ptp clock</b>	Displays the properties of the local clock.
	<b>show ptp clocks foreign-masters-record</b>	Displays the state of foreign masters known to the PTP process.
	<b>show ptp delay</b>	Displays the link delay and residence delay status of the PTP interface.
	<b>show ptp parent</b>	Displays the properties of the PTP parent.
	<b>show ptp port</b>	Displays the status of the PTP port.
	<b>show ptp time-property</b>	Displays the properties of the PTP clock.

# show ptp delay

To display the link delay and residence delay status of the Precision Time Protocol (PTP) interfaces, use the **show ptp delay** command.

## show ptp delay summary

Syntax	Description
<b>interface</b>	Specifies an interface.
<b>ethernet slot/port</b>	(Optional) Specifies an Ethernet interface.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	5.2(1)	This command was introduced.
	7.3(0)D1(1)	This command was modified. The field <i>RD</i> , indicating Residence Delay, has been added to the output.

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

**Examples** This example shows how to display the link delay and residence delay status of the PTP interfaces. The output indicates the measured link delay and the configured residence delay, nanoseconds. The field descriptions are self-explanatory.

```
switch# show ptp delay summary
```

Legend:

PM(Port mode): BC-Boundary Clock, TC-Transparent Clock, GP-Generalized PTP

PS(Port state): M-Master, S-Slave, P-Passive, D-Disabled, C-Uncalibrated

LD: Link Delay

RD: Residence Delay

```
-----  
Interface PM PS LD(ns) RD(ns)  
-----
```

```
Eth1/1 GP M 220 5000
```

```
Eth1/15 GP S 204 5000
```

```
Eth1/31 GP M 360 5000
```

```
Eth1/32 GP M 516 5000
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ptp clock</b>	Displays the properties of the local clock.
<b>show ptp clocks foreign-masters-record</b>	Displays the state of foreign masters known to the PTP process.
<b>show ptp counters</b>	Displays PTP specific packet counters for all Ethernet interfaces or for a specified interface.
<b>show ptp corrections</b>	Displays the last few PTP corrections.
<b>show ptp parent</b>	Displays the properties of the PTP parent.
<b>show ptp port</b>	Displays the status of the PTP port.
<b>show ptp time-property</b>	Displays the properties of the PTP clock.



# 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.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	5.2(1)	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
Parent Clock:
Parent Clock Identity:  0:18:ba:ff:ff:d8: e:16
Parent Port Number: 1546
Observed Parent Offset (log variance): N/A
Observed Parent Clock Phase Change Rate: N/A

Grandmaster Clock:
Grandmaster Clock Identity:  0:18:ba:ff:ff:d8: e:16
Grandmaster Clock Quality:
  Class: 248
  Accuracy: 254
  Offset (log variance): 65535
  Priority1: 255
  Priority2: 255
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ptp brief</b>	Displays the PTP status.
	<b>show ptp clock</b>	Displays the properties of the local clock.
	<b>show ptp clocks foreign-masters-record</b>	Displays the state of foreign masters known to the PTP process.
	<b>show ptp counters</b>	Displays PTP specific packet counters for all Ethernet interfaces or for a specified interface.
	<b>show ptp corrections</b>	Displays the last few PTP corrections.
	<b>show ptp port</b>	Displays the status of the PTP port.
	<b>show ptp time-property</b>	Displays the properties of the PTP clock.

# show ptp port

To display information about the Precision Time Protocol (PTP) port, use the **show ptp port** command.

```
show ptp port {interface [ethernet]}
```

Syntax Description	Parameter	Description
	<b>interface</b>	Specifies the interface.
	<b>ethernet</b>	(Optional) Specifies an Ethernet interface.

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	5.2(1)	This command was introduced.
	7.3(0)DX(1)	This command was modified. The fields <i>Port mode</i> , <i>Port encapsulation</i> , and <i>PTP vlan</i> have been added to the output.

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

**Examples** This example shows how to display information about the PTP port:

```
switch# show ptp port interface ethernet 5/1
PTP Port Dataset: Eth5/1
Port identity: clock identity: 8c:60:4f:ff:fe:88:ae:42
Port identity: port number: 1024
PTP version: 2
Port state: Slave
Port mode: generalized-PTP
Port encapsulation: layer-2
PTP vlan: 1
Delay request interval(log mean): 2
Announce receipt time out: 3
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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ptp brief</b>	Displays the PTP status.
	<b>show ptp clock</b>	Displays the properties of the local clock.
	<b>show ptp clocks foreign-masters-record</b>	Displays the state of foreign masters known to the PTP process.
	<b>show ptp counters</b>	Displays PTP specific packet counters for all Ethernet interfaces or for a specified interface.
	<b>show ptp corrections</b>	Displays the last few PTP corrections.
	<b>show ptp parent</b>	Displays the properties of the PTP parent.
	<b>show ptp time-property</b>	Displays the properties of the PTP clock.

# 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.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	5.2(1)	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: 33
  Leap59: 0
  Leap61: 0
  Time Traceable: 0
  Frequency Traceable: 0
  PTP Timescale: 0
  Time Source: 0xA0(internal Oscillator)
```

Related Commands	Command	Description
	<b>show ptp brief</b>	Displays the PTP status.
	<b>show ptp clock</b>	Displays the properties of the local clock.
	<b>show ptp clocks foreign-masters-record</b>	Displays the state of foreign masters known to the PTP process.

<b>Command</b>	<b>Description</b>
<b>show ptp counters</b>	Displays PTP specific packet counters for all Ethernet interfaces or for a specified interface.
<b>show ptp corrections</b>	Displays the last few PTP corrections.
<b>show ptp parent</b>	Displays the properties of the PTP parent.
<b>show ptp port</b>	Displays the status of the PTP port.

# show redundancy status

To show detailed information about redundancy, use the **show redundancy status** command.

## show redundancy status

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to displays redundancy information:

```
switch# show redundancy status
Redundancy mode
-----
      administrative:  HA
      operational:    None

This supervisor (sup-6)
-----
      Redundancy state:  Active
      Supervisor state:  Active
      Internal state:   Active with no standby

Other supervisor (sup-5)
-----
      Redundancy state:  Not present

      Supervisor state:  N/A
      Internal state:   N/A

System start time:          Fri Aug 15 15:55:19 2008

System uptime:              3 days, 23 hours, 57 minutes, 22 seconds
```

## ■ show redundancy status

```
Kernel uptime:          4 days, 0 hours, 1 minutes, 39 seconds
Active supervisor uptime: 3 days, 23 hours, 57 minutes, 22 secondss
```



# show resource monitor-session

To display the resources that are available for a traditional Ethernet Switched Port Analyzer (SPAN) session, use the **show resource monitor-session** command.

## show resource monitor-session

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	6.2(2)	This command was introduced.

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

**Examples** This example shows how to display the resources that are available for traditional SPAN sessions:

```
switch# show resource monitor-session
Resource           Min      Max      Used      Unused      Avail
-----
monitor-session    0        2        0         0           2
```

Related Commands	Command	Description
	<b>show resource monitor-session-extended</b>	Displays the resources that are available for an extended SPAN and ERSPAN session.

# show resource monitor-session-extended

To display the resources that are available for the extended Ethernet Switched Port Analyzer (SPAN) or Encapsulated Remote Switched Port Analyzer (ERSPAN) sessions, use the **show resource monitor-session-extended** command.

**show resource monitor-session-extended**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	6.2(2)	This command was introduced.

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

**Examples** This example shows how to display the resources that are available for extended SPAN or ERSPAN sessions:

```
switch# show resource monitor-session-extended
```

Resource	Min	Max	Used	Unused	Avail
-----	---	---	----	-----	-----
monitor-session-extended	0	12	0	0	12

Related Commands	Command	Description
	<b>show resource monitor-session</b>	Displays the resources that are available for a traditional SPAN session.

# show rmon

To display the configuration or onboard logs, use the **show rmon** command.

```
show rmon {alarms | events | hcalarms | logs | status}
```

Syntax Description		
<b>alarms</b>		Displays the configured 32-bit RMON alarms.
<b>events</b>		Displays the configured RMON events.
<b>hcalarms</b>		Displays the configured 64-bit HC (High Capacity) RMON alarms.
<b>logs</b>		Displays the RMON event log.
<b>status</b>		Displays the RMON information.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the configured RMON alarms:

```
switch# show rmon alarms
Alarm 20 is active, owned by test
Monitors 1.3.6.1.2.1.2.2.1.16.30 every 30 second(s)
Taking delta samples, last value was 17
Rising threshold is 15, assigned to event 1
Falling threshold is 0, assigned to event 0
On startup enable rising or falling alarm
```

This example shows how to display the configured RMON events:

```
switch# show rmon events
Event 4 is active, owned by administrator@london_op_center
Description is WARNING(4)
Event firing causes log and trap to community public, last fired 03:32:43
```

This example shows how to display the configured high-capacity RMON alarms:

```
switch# show rmon hcalarms
High Capacity Alarm 1 is active, owned by cseSysCPUUtilization.0@test
Monitors 1.3.6.1.4.1.9.9.305.1.1.1.0 every 10 second(s)
Taking absolute samples, last value was 0
Rising threshold is 60, assigned to event 4
Falling threshold is 59, assigned to event 4
On startup enable rising alarm
```

This example shows how to display RMON configuration and logged information:

```
switch# show rmon status
Maximum allowed 32 bit or 64 bit alarms : 512
Number of 32 bit alarms configured : 0
Number of 64 bit hcalarms configured : 0
switch#
```

#### Related Commands

Command	Description
<b>rmon alarm</b>	Configures the 32-bit RMON alarm.
<b>rmon event</b>	Configures an RMON event.
<b>rmon hcalarm</b>	Configures the 64-bit RMON alarm.

# show run mmode

To display the currently running maintenance profile configuration on a switch, use the **show run mmode** command.

**show run mmode [all]**

<b>Syntax Description</b>	<b>all</b>	Displays the currently running maintenance profile configuration along with the defaults.
---------------------------	------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.3(0)D1(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display the currently running maintenance profile configuration on a switch:
-----------------	--

```
switch(config)# show run mmode

!Command: show running-config mmode
!Time: Wed May 13 22:37:02 1970

version 7.3(0)D1(1)
configure maintenance profile normal-mode
  router isis 100
    no isolate
  router ospf 100
    no isolate
  router bgp 100
    no isolate
configure maintenance profile maintenance-mode
  router bgp 100
    isolate
  router ospf 100
    isolate
  router isis 100
```

```

    isolate
configure terminal

```

Related Commands	Command	Description
	<b>configure maintenance profile</b>	Enters a maintenance profile configuration session to create a custom maintenance mode profile or a custom normal mode profile.
	<b>show system mode</b>	Displays the current system mode and the current state of the maintenance mode timer when the switch is in maintenance mode.
	<b>system mode maintenance always-use-custom-profile</b>	Applies the existing custom maintenance mode profile and prevents creation of auto-generated maintenance mode profile.
	<b>system mode maintenance on-reload reset-reason</b>	Boots the switch into maintenance mode automatically in the event of a specified system crash.
	<b>system mode maintenance shutdown</b>	Shuts down all protocols and interfaces except the management interface (by using the <b>shutdown</b> command and not the default <b>isolate</b> command).
	<b>system mode maintenance timeout</b>	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

# show running-config cdp

To display the Cisco Discovery Protocol (CDP) running configuration, use the **show running-config cdp** command.

**show running-config cdp [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays the running configuration with defaults.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>Supported User Roles</b>	network-admin network-operator vdc-admin vdc-operator
-----------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display the CDP running configuration with defaults:

```
switch(config)# show running-config cdp all
!Command: show running-config cdp all
!Time: Fri Jan 15 22:19:20 2010
```

```
version 5.0(2)
logging level cdp 6
cdp advertise v2
cdp enable
cdp holdtime 180
cdp timer 60
cdp format device-id system-name
```

```
interface Ethernet6/1
  cdp enable
```

```
interface Ethernet6/2
  cdp enable
```

```
interface Ethernet6/3
```

```

    cdp enable

interface Ethernet6/4
  cdp enable

interface Ethernet6/5
  cdp enable

interface Ethernet6/6
  cdp enable

interface Ethernet6/7
  cdp enable

interface Ethernet6/8
  cdp enable

interface Ethernet7/1
  cdp enable

interface Ethernet7/2
  cdp enable

interface Ethernet7/3
  cdp enable

interface Ethernet7/4
  cdp enable

interface Ethernet7/5
  cdp enable

interface Ethernet7/6
  cdp enable

interface Ethernet7/7
  cdp enable

interface Ethernet7/8
  cdp enable
--More--
switch(config)#

```

**Related Commands**

Command	Description
<b>enable cdp</b>	Enables CDP on an interface.



# show running-config diagnostic

To display the running-configuration diagnostics, use the **show running-config diagnostic** command.

**show running-config diagnostic [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays the running-configuration diagnostics with defaults.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display the running-configuration diagnostics:
-----------------	--

```
switch(config)# show running-config diagnostic all

!Command: show running-config diagnostic all
!Time: Fri Jan 15 22:22:01 2010

version 5.0(2)
diagnostic bootup level complete

switch(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show startup-config diagnostic</b>	Displays the startup-configuration diagnostics.

# show running-config eem

To display the Embedded Event Manager (EEM) running configuration, 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

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows the Embedded Event Manager (EEM) running configuration:

```
switch# show running-config eem
switch(config)# show running-config eem

!Command: show running-config eem
!Time: Fri Jan 15 22:23:28 2010

version 5.0(2)

switch(config)#
```

# show running-config lldp

To display the global Link Layer Discovery Protocol (LLDP) configuration, use the **show running-config lldp** command.

**show running-config lldp**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the global LLDP configuration:

```
switch(config)# show running-config lldp

!Command: show running-config lldp
!Time: Mon Jan 11 02:19:29 2010

version 5.0(2)
feature lldp

logging level lldp 5

switch(config)#
```

Related Commands	Command	Description
	<b>feature lldp</b>	Enables the LLDP feature globally.

# show running-config monitor

To display information about the running Ethernet Switched Port Analyzer (SPAN) configuration on the system, use the **show running-config monitor** command.

**show running-config monitor [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays the running SPAN configuration with defaults.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display the running SPAN configuration on the system:

```
switch(config)# show running-config monitor
!Command: show running-config monitor
!Time: Fri Jan 15 22:24:43 2010

version 5.0(2)
logging level monitor 6
switch(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show monitor</b>	Displays information about the SPAN configuration.
	<b>show startup-config monitor</b>	Displays information about the startup SPAN configuration.

# show running-config netflow

To display the NetFlow configuration that is currently on your switch, use the **show running-config netflow** command.

**show running-config netflow [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays the NetFlow configuration with defaults.				
<b>Defaults</b>	None				
<b>Command Modes</b>	Any command mode				
<b>Supported User Roles</b>	network-admin network-operator vdc-admin vdc-operator				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
<b>Usage Guidelines</b>	This command does not require a license.				

**Examples**

This example shows how to display the NetFlow configuration that is running on the switch:

```
switch(config)# show running-config netflow all
!Command: show running-config netflow all
!Time: Fri Jan 15 22:26:04 2010

version 5.0(2)
feature netflow

flow timeout active 1800
flow timeout inactive 15
flow exporter new_flow_1
  transport udp 9995
  dscp 0
  version 5
flow exporter new_flow_2
  transport udp 9995
  dscp 0
  version 9
  template data timeout 1800
flow exporter test
  transport udp 9995
  dscp 0
  version 9
  template data timeout 1800
flow exporter Custom-Flow-Exporter-1
  transport udp 9995
  dscp 0
  version 9
  template data timeout 1800
  option exporter-stats timeout 1200
switch(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show startup-config netflow</b>	Displays the startup NetFlow configurations.

# show running-config ntp

To display the Network Time Protocol (NTP) configuration that is currently running on the system, use the **show running-config ntp** command.

**show running-config ntp [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays all of the NTP running configuration.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display the NTP configuration that is currently running:

```
switch(config)# show running-config ntp

!Command: show running-config ntp
!Time: Fri Jan 15 22:28:34 2010

version 5.0(2)
ntp server 190.0.2.10
ntp server 192.0.2.10 prefer use-vrf RED key 786
ntp peer 2001:db8::4101
ntp authentication-key 3 md5 fewhg 7
ntp authentication-key 34567 md5 qabzk7f 7
ntp logging
ntp access-group peer abcd*123

switch(config)#
```

## ■ show running-config ntp

Related Commands	Command	Description
	<b>show ntp source-interface</b>	Displays information about the NTP source interface.
	<b>show startup-config ntp</b>	Displays information about the startup NTP configuration of the switch.



# show running-config snmp

To display the running Simple Network Management Protocol (SNMP) configuration of a system, use the **show running-config snmp** command.

**show running-config snmp [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays the running SNMP configuration with defaults.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display the running SNMP configuration of a system:

```
switch(config)# show running-config snmp
!Command: show running-config snmp
!Time: Fri Jan 15 22:30:27 2010

version 5.0(2)
snmp-server user admin network-admin auth md5 0x1dc65f45a9d8e41dbccd76380946d6c3
priv 0x1dc65f45a9d8e41dbccd76380946d6c3 localizedkey

switch(config)#
```

<b>Related Commands!</b>	<b>Command</b>	<b>Description</b>
	<b>show startup-config snmp</b>	Displays the startup SNMP configuration.
	<b>show port-monitor active</b>	Displays active port-monitor policies.

# show sampler

To display a NetFlow sampler, use the **show sampler** command.

```
show sampler [name] [sampler-name]
```

Syntax Description	name	(Optional) Specifies a sampler.
	<i>sampler-name</i>	(Optional) Sampler name. The maximum number of characters is 32.

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

Command Modes	Any command mode
---------------	------------------

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

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

Usage Guidelines	You can create a sampler to define the NetFlow sampling rate for a flow. This command does not require a license.
------------------	--

Examples	This example shows how to display a NetFlow sampler:  <pre>switch(config)# <b>show sampler</b> Sampler Netflow-Sampler-1:   mode 1 out-of 1000 switch(config)#</pre>
----------	--

Related Commands	Command	Description
	<b>sampler</b>	Configures a sampler to collect data for a user selected packet ratio to preserve hardware resources.

# show scheduler

To display information about scheduled maintenance jobs, use the **show scheduler** command.

```
show scheduler { config | internal [mem-stats] | job [name jobname] | logfile | schedule [name
  schedulename]}
```

Syntax Description		
<b>config</b>		Displays scheduler configuration information.
<b>internal</b>		Provides the internal scheduler information as specified.
<b>mem-stats</b>		(Optional) Provides the scheduler internal memory information as specified.
<b>job</b>		Displays job information as specified.
<b>name jobname</b>		(Optional) Displays information for the specified scheduler job name.
<b>logfile</b>		Displays the scheduler log file as specified.
<b>schedule</b>		Displays the scheduler timetable as specified.
<b>name schedulename</b>		(Optional) Displays the scheduler timetable for the specified schedule name.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines**

To use this command, the scheduler must already be enabled.

To enable the scheduler, use the **feature scheduler** command.

This command does not require a license.

**Examples** This example shows how to display the scheduler configuration:

```
switch# show scheduler config
config terminal
  feature scheduler
  scheduler logfile size 16
```

```

end

config terminal
  scheduler job name test-1
end

config terminal
  scheduler job name test
end

config terminal
  scheduler job name test1
end

config terminal
  scheduler job name test2
end

switch#

```

This example shows how to display the specified scheduler timetable:

```

switch# show scheduler schedule name test
Schedule Name : test
-----
User Name : admin
Schedule Type : Run once on Tue Aug 10 09:48:00 2008
Last Execution Time: Tue Aug 10 09:48:00 2008
-----
Job Name      Status
-----
addMem       Success (0)

```

#### Related Commands

Command	Description
<b>scheduler</b>	Configures maintenance jobs.
<b>feature scheduler</b>	Enables the scheduler feature for scheduling maintenance jobs.

# show snapshots

To display the snapshots present on the switch, use the **show snapshots** command.

## show snapshots

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

**Defaults** None

**Command Modes** Privileged EXEC

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	7.2(0)	This command was introduced.

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

**Examples** This example shows how to display the snapshots present on the switch:

```
switch# show snapshots
Snapshot Name          Time                Description
-----
before_maintenance    Wed May 13 13:21:16 1970  system-internal-snapshot
new                   Mon May 11 15:51:27 1970  after if down
```



### Note

In the above output example, “before\_Maintenance” is the system-generated snapshot and “new” is the user-generated snapshot.

Related Commands	Command	Description
	<b>snapshot create</b> <i>name</i> <i>description</i>	Creates a snapshot. The name variable can be 64 characters in length. The description variable can be 256 characters in length.
	<b>snapshot delete</b>	Deletes a snapshot.
	<b>show snapshots compare</b>	Displays the comparison between two snapshots.

<b>Command</b>	<b>Description</b>
<b>show snapshots dump</b>	Displays content of the various sections in a generated snapshot.
<b>snapshot section</b>	Adds or deletes a snapshot section.

# show snapshots compare

To display the comparison between the two snapshots on a switch, use the **show snapshots compare** command.

```
show snapshots snapshot-1 snapshot-2 [ipv4routes | ipv6routes | summary]
```

Syntax Description		
	<i>snapshot-1</i>	Displays the comparison between the two snapshots.
	<i>snapshot-2</i>	
	<b>ipv4routes</b>	Displays a comparison of the IPv4 routes between the two snapshots.
	<b>ipv6routes</b>	Displays a comparison of the IPv6 routes between the two snapshots.
	<b>summary</b>	Displays a summary of the comparison between the two snapshots.

**Defaults** None

**Command Modes** Privileged EXEC

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	7.2(0)	This command was introduced.

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

**Examples**

This example shows how to display a comparison between two snapshots:

```
switch# show snapshots compare before_maint during_maint

=====
Feature          Tag          before_maint    during_maint
=====
[bgp]
-----

[eigrp]
-----

[eigrpv6]
-----

[interface]
-----

... <snip> ...

[v4route]
-----

      [ipprefix:0.0.0.0/32]
            uptime          PT24M32S          **PT58M37S**

      [ipprefix:127.0.0.0/8]
            uptime          PT24M32S          **PT58M37S**
```

This example shows how to display a summary of the comparison between two snapshots:

```
switch# show snapshots compare before_maintenance after_maintenance summary

=====
Feature          before_maintenance after_maintenance
changed
=====
basic summary
# of interfaces          50          50
# of vlans                0           0
# of ipv4 routes vrf default  13         13
# of ipv4 paths vrf default  13         13
# of ipv4 routes vrf management 14         14
# of ipv4 paths vrf management 14         14
# of ipv6 routes vrf default   3           3
# of ipv6 paths vrf default   3           3

interfaces
# of eth interfaces      48          48
# of eth interfaces up   1           1
# of eth interfaces down 47          47
# of eth interfaces other 0           0

# of vlan interfaces     0           0
# of vlan interfaces up  0           0
# of vlan interfaces down 0           0
# of vlan interfaces other 0           0
```

This example shows how to display a comparison of the IPv4 routes between the two snapshots:

```
switch# show snapshots compare snapshot1 snapshot2 ipv4routes
```



## Related Commands

Command	Description
<b>show snapshots</b>	Displays snapshots on a switch.
<b>show snapshots dump</b>	Display content of the various sections in a generated snapshot.
<b>show snapshots sections</b>	Displays content of the various sections in a generated snapshot.
<b>snapshot create</b> <i>name</i> <i>description</i>	Creates a snapshot. The name variable can be 64 characters in length. The description variable can be 256 characters in length.
<b>snapshot delete</b>	Deletes a snapshot.
<b>show snapshots dump</b>	Displays content of the various sections in a generated snapshot.
<b>snapshot section</b>	Adds or deletes a snapshot section.

# show snapshots dump

To display content of the various sections in a generated snapshot, use the **show snapshots dump** command.

**show snapshots dump** *snapshot-name*

<b>Syntax Description</b>	<i>snapshot-name</i> Name of the snapshot.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.3(0)D1(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	The following example shows how to display content of the various sections in a generated snapshot:
-----------------	---

```
switch# show snapshots dump new

File: interface.xml      Snapshot: new
=====
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:7.3.0.D1.1.:if_manager">
  <nf:data>
    <show>
      <interface>
        <__readonly__>
          <TABLE_interface>
            <ROW_interface>
              <interface>mgmt0</interface>
              <state>up</state>
              <admin_state>up</admin_state>
              <eth_hw_desc>GigabitEthernet</eth_hw_desc>
              <eth_hw_addr>5cfc.666d.3b34</eth_hw_addr>
              <eth_bia_addr>5cfc.666d.3b34</eth_bia_addr>
              <eth_ip_addr>5.24.100.101</eth_ip_addr>
            </ROW_interface>
          </TABLE_interface>
        </__readonly__>
      </interface>
    </show>
  </nf:data>
</nf:rpc-reply>
```

```
<eth_ip_mask>16</eth_ip_mask>  
<eth_ip_prefix>5.24.0.0</eth_ip_prefix>  
<eth_mtu>1500</eth_mtu>
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show snapshots</b>	Displays snapshots on a switch.
<b>show snapshots sections</b>	Displays content of the various sections in a generated snapshot.
<b>snapshot create</b> <i>name</i> <i>description</i>	Creates a snapshot. The name variable can be 64 characters in length. The description variable can be 256 characters in length.
<b>snapshot delete</b>	Deletes a snapshot.
<b>show snapshots dump</b>	Displays content of the various sections in a generated snapshot.
<b>snapshot section</b>	Adds or deletes a snapshot section.

# show snapshots sections

To display the user-specified sections in a snapshot, use the **show snapshots sections** command.

## show snapshots sections

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

**Defaults** None

**Command Modes** Privileged EXEC

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

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

**Examples** This example shows how to display the user-specified sections in a snapshot:

```
switch# show snapshots sections
user-specified snapshot sections
-----
[v4route]
show command: show ip route detail vrf all
row id: ROW_prefix
key1: ipprefix
key2: -
```

Related Commands	Command	Description
	<b>show snapshots compare</b>	Displays the comparison between two snapshots.
	<b>show snapshots dump</b>	Displays content of the various sections in a generated snapshot.
	<b>snapshot create <i>name</i> <i>description</i></b>	Creates a snapshot. The name variable can be 64 characters in length. The description variable can be 256 characters in length.

<b>Command</b>	<b>Description</b>
<b>snapshot delete</b>	Deletes a snapshot.
<b>snapshot section</b>	Adds or deletes a snapshot section.

# show snmp

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

**show snmp**

---

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

---

**Defaults** None

---

**Command Modes** Any command mode

---

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

---

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

---



---

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

**Examples**

This example shows how to display the SNMP information:

```

switch(config)# show snmp
sys contact:
sys location: anyplace, Anywhere

0 SNMP packets input
  0 Bad SNMP versions
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors
  0 No such name errors
  0 Bad values errors
  0 General errors

Community                               Group / Access
-----
Comm2                                    network-admin
testCommunity                            vdc-operator
com3                                       vdc-admin

-----
SNMP USERS
-----

User           Auth  Priv(enforce)  Groups
-----
foo            md5   aes-128(no)   network-operator
               vdc-admin
               network-admin
User3          md5   no             network-operator
admin          md5   des(no)       network-admin
user1          md5   des(no)       vdc-admin

NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----

User           Auth  Priv
-----
foo            md5   no
(EngineID 11:22:33:44:55)

foo            sha   no
(EngineID 33:0:33:22:33)

SNMP Tcp Authentication Flag : Enabled.
    
```

■ show snmp

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>snmp-server community</b>	Configures SNMP community strings.



# show snmp community

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

**show snmp community**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** Use the **show snmp community** command to display a list of SNMP communities configured on a device.

In Cisco NX-OS Release 4.0(2) and later releases, the **show snmp-community** command displays any SNMP contexts that are mapped to SNMPv2c communities.

This command does not require a license.

**Examples** This example shows how to display the SNMP community strings and any associated SNMP contexts:

```
switch# show snmp community
Community                Group / Access  context
-----                -
testCommunity            vdc-operator   contextB
Comm2                     network-admin
com3                      vdc-admin
```

## ■ show snmp community

Related Commands	Command	Description
	<b>snmp-server community</b>	Configures SNMP community strings.
	<b>snmp-server mib community-map</b>	Maps SNMP community strings to SNMP contexts.

# show snmp context

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

**show snmp context**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.0(2)	This command was introduced.

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

**Examples** This example shows how to display the SNMP context mapping:

```
switch# show snmp context
-----
Context                               [Protocol instance, VRF, Topology]
-----
contextB                               instancel,
                                         vrf1,
                                         topol
-----
```

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

# show snmp engineID

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

## show snmp engineID

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

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

```
switch(config)# show snmp engineID
Local SNMP engineID: [Hex] 80000009030005300A0B0C
                    [Dec] 128:000:000:009:003:000:005:048:010:011:012
```

Related Commands	Command	Description
	snmp-server user	Configures SNMP target notification users.

# show snmp group

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

## **show snmp group**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

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

**Examples**

This example shows how to display the SNMP groups:

```
switch(config)# show snmp group

role: network-admin
description: Predefined network admin role has access to all commands
on the switch
-----
Rule    Perm    Type    Scope    Entity
-----
1       permit read-write

role: network-operator
description: Predefined network operator role has access to all read
commands on the switch
-----
Rule    Perm    Type    Scope    Entity
-----
1       permit read

role: vdc-admin
description: Predefined vdc admin role has access to all commands within
a VDC instance
-----
Rule    Perm    Type    Scope    Entity
-----
1       permit read-write

role: vdc-operator
description: Predefined vdc operator role has access to all read commands
within a VDC instance
-----
Rule    Perm    Type    Scope    Entity
-----
1       permit read
```

**Related Commands**

Command	Description
role name	Configures security roles used as SNMP groups.

# show snmp host

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

**show snmp host**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the SNMP hosts:

```
switch(config)# show snmp host
-----
Host                               Port Version  Level  Type  SecName
-----
192.0.2.1                          33   v1       noauth trap  Comm2
-----
192.0.2.2                          162  v3       auth   trap  comm3
-----
Use VRF: Blue
-----
192.0.2.10                         162  v3       auth   trap  testCommunity
-----
Filter VRF: Red
-----
```

■ show snmp host

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>snmp-server host</b>	Configures SNMP hosts.



# 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.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the SNMP sessions:

```
switch(config)# show snmp sessions
```

Related Commands	Command	Description
	<b>snmp-server user</b>	Configures SNMP users.

# show snmp source-interface

To display the Simple Network Management Protocol (SNMP) source interface through which notifications are sent, use the **show snmp source-interface** command.

## show snmp source-interface

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

**Defaults** None

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.2(1)	This command was introduced.

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

**Examples** This example shows how to display the SNMP source interface through which notifications are sent:

```
switch(config)# show snmp source-interface
-----
Notification                source-interface
-----
trap                          lookback1
inform                        Ethernet1/1
-----
switch(config)#
```

Related Commands	Command	Description
	<b>snmp-server source-interface</b>	Configures an SNMP source interface through which notifications are sent.

# show snmp trap

To display the Simple Network Management Protocol (SNMP) notification enable status, use the **show snmp trap** command.

**show snmp trap**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the SNMP notification enable status:

```
switch(config)# show snmp trap
Trap type           Enabled
-----
aaa server state-change      No
callhome                   No
entity fru                  Yes
license                     Yes
snmp authentication         No
vrrp                        No
link                        No
bridge topologychange       No
bridge newroot              No
stp inconsistency           No
stp loop-inconsistency      No
stp root-inconsistency      No
```

■ show snmp trap

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>snmp-server trap enable</b>	Enables SNMP notifications.

# show snmp user

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

```
show snmp user [username [engineID id]]
```

Syntax Description		
<i>username</i>	(Optional) Name of the user. The name can be any case-sensitive, alphanumeric string up to 32 characters.	
<b>engineID</b> <i>id</i>	(Optional) Configures the SNMP Engine ID for a notification target user. The ID is 11 decimal values separated by colons.	

Defaults	
	Displays all users

Command Modes	
	Any command mode

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

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

Usage Guidelines	
	This command does not require a license.

**Examples**

This example shows how to display the SNMP users:

```
switch(config)# show snmp user
```

```

SNMP USERS
-----
User                Auth  Priv(enforce) Groups
-----
foo                 md5   aes-128(no)   network-operator
                  vdc-admin
                  network-admin
User3
admin              md5   no            network-operator
user1              md5   des(no)       network-admin
                  vdc-admin
-----
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
User                Auth  Priv
-----
foo                 md5   no
(EngineID 11:22:33:44:55)

```

**Related Commands**

Command	Description
<b>snmp-server user</b>	Configures SNMP users.

# show sprom

To display the contents of the serial PROM (SPROM) on the device, use the **show sprom** command.

```
show sprom {all | backplane bp-number | clock clock-number | cmp | fan fan-number | module slot
| powersupply ps-number | stby-sup | sup | xbar xbar-number}
```

Syntax Description		
<b>all</b>		Displays the SPROM contents for all components on the physical device.
<b>backplane</b> <i>bp-number</i>		Displays the SPROM contents for a backplane.
<b>clock</b> <i>clock-number</i>		Displays the SPROM contents for a clock module.
<b>cmp</b>		Displays the SPROM contents for a Connectivity Management Processor (CMP).
<b>fan</b> <i>fan-number</i>		Displays the SPROM contents for a fan.
<b>module</b> <i>slot</i>		Displays the SPROM contents for a I/O module.
<b>powersupply</b> <i>ps-number</i>		Displays the SPROM contents for a power supply.
<b>stby-sup</b>		Displays the SPROM contents for the standby supervisor module.
<b>sup</b>		Displays the SPROM contents for the active supervisor module.
<b>xbar</b> <i>xbar-number</i>		Displays the SPROM contents for a fabric module.

**Defaults** Displays summary information for all processes on the device.

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

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

**Usage Guidelines** The SPROM on the physical device components contain detailed information about the hardware, including the serial number, part number, and revision numbered.

This command does not require a license.

**Examples**

This example shows how to display SPROM information for all components on the physical device:

```
switch# show sprom all
DISPLAY active supervisor sprom contents:
Common block:
  Block Signature : 0xabab
  Block Version  : 3
  Block Length   : 160
  Block Checksum : 0x158a
  EEPROM Size    : 65535
  Block Count    : 3
  FRU Major Type : 0x6004
  FRU Minor Type : 0x5
  OEM String     : Cisco Systems, Inc
  Product Number : N7K-SUP1
  Serial Number  : JAB10380101
  Part Number    : 73-10877-03
  Part Revision  : 09
  Mfg Deviation  : 0
  H/W Version    : 0.311
  Mfg Bits       : 0
  Engineer Use   : 0
  snmpOID        : 0.0.0.0.0.0.0.0
  Power Consump  : -247
  RMA Code       : 0-0-0-0
  CLEI Code      : TBD
  VID            : TBD
...
```

This example shows how to display SPROM information for a backplane:

```
switch# show sprom backplane 1
DISPLAY backplane sprom contents:
Common block:
  Block Signature : 0xabab
  Block Version  : 3
  Block Length   : 160
  Block Checksum : 0x147e
  EEPROM Size    : 65535
  Block Count    : 5
  FRU Major Type : 0x6001
  FRU Minor Type : 0x0
  OEM String     : Cisco Systems, Inc.
  Product Number : N7K-C7010
  Serial Number  : TBM11256507
  Part Number    : 73-10900-04
  Part Revision  : 03
  Mfg Deviation  :
  H/W Version    : 0.403
  Mfg Bits       : 0
  Engineer Use   : 0
  snmpOID        : 0.0.0.0.0.0.0.0
  Power Consump  : -247
  RMA Code       : 0-0-0-0
  CLEI Code      :
  VID            :
Chassis specific block:
  Block Signature : 0x6001
  Block Version  : 3
  Block Length   : 39
  Block Checksum : 0x3bf
  Feature Bits   : 0x0
  HW Changes Bits : 0x0
```



```

Stackmib OID      : 0
MAC Addresses     : 00-18-ba-d8-3f-bc
Number of MACs    : 128
OEM Enterprise    : 9
OEM MIB Offset    : 5
MAX Connector Power: 1
WWN software-module specific block:
Block Signature   : 0x6005
Block Version     : 1
Block Length      : 0
Block Checksum    : 0x66
wwn usage bits:
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00
License software-module specific block:
Block Signature   : 0x6006
Block Version     : 1
Block Length      : 16
Block Checksum    : 0x77
lic usage bits:
00 00 00 00 00 00 00 00
Second Serial number specific block:
Block Signature   : 0x6007
Block Version     : 1
Block Length      : 28
Block Checksum    : 0x302
Serial Number     : TBM11256507

```

# show startup-config cdp

To display the Cisco Discovery Protocol (CDP) startup configuration, use the **show startup-config cdp** command.

**show startup-config cdp [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays the startup configuration with defaults.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.1(2)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display the CDP startup configuration with defaults:
-----------------	--

```
switch(config)# show startup-config cdp all
!Command: show startup-config cdp
!Time: Tue Feb  2 22:36:26 2010

version 5.0(2)
logging level cdp 6

switch(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show running-config cdp</b>	Displays the running CDP configuration.

# show startup-config diagnostic

To display startup-configuration diagnostics, use the **show startup-config diagnostic** command.

**show startup-config diagnostic [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays the startup configuration with defaults.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	<p>This example shows how to display the startup-configuration diagnostics:</p> <pre>switch(config)# show startup-config diagnostic all !Command: show startup-config diagnostic all !Time: Tue Jan 26 22:38:22 2010 !Startup config saved at: Thu Jan 21 08:39:42 2010  version 5.0(2) diagnostic bootup level complete  switch(config)#</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show running-config diagnostic</b>	Displays the running-configuration diagnostics.

# show startup-config cfs

To display information about the Cisco Fabric Services (CFS) startup configuration, use the **show startup-config cfs** command.

**show startup-config cfs [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays all of the CFS startup configuration.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>Supported User Roles</b>	network-admin network-operator vdc-admin vdc-operator
-----------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.1(2)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display the CFS startup configuration:

```
switch(config)# show startup-config cfs

!Command: show startup-config cfs
!Time: Tue Feb 2 22:40:47 2010
!Startup config saved at: Thu Jan 21 08:39:42 2010

version 5.0(2)
switch(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cfs distribute</b>	Enables CFS distribution for the device globally.
	<b>show cfs status</b>	Displays the CFS distribution status.

# show startup-config eem

To display the Embedded Event Manager (EEM) startup configuration, 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

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the Embedded Event Manager (EEM) startup configuration:

```
switch# show startup-config eem
!Command: show startup-config eem
!Time: Tue Feb  2 22:41:25 2010
!Startup config saved at: Thu Jan 21 08:39:42 2010

version 5.0(2)
switch#
```

# show startup-config monitor

To display information about the startup Ethernet Switched Port Analyzer (SPAN) configuration, use the **show startup-config monitor** command.

**show startup-config monitor**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.0(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 Ethernet SPAN configuration:

```
switch(config)# show startup-config monitor
!Command: show startup-config monitor
!Time: Tue Feb  2 22:42:07 2010
!Startup config saved at: Thu Jan 21 08:39:42 2010

version 5.0(2)
logging level monitor 6
switch(config)#
```

Related Commands	Command	Description
	<b>show monitor</b>	Displays information about an Ethernet Switched Port Analyzer (SPAN).
	<b>show running-config monitor</b>	Displays the running configuration to the startup configuration.

# show startup-config netflow

To display the startup NetFlow configuration, use the **show startup-config netflow** command.

**show startup-config netflow [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays the startup NetFlow configuration with defaults.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display the startup NetFlow configuration:
-----------------	--

```
switch# show startup-config netflow

!Command: show startup-config monitor
!Time: Tue Feb  2 22:42:07 2010
!Startup config saved at: Thu Jan 21 08:39:42 2010

version 5.0(2)
logging level monitor 6

switch(config)# show startup-config netflow

!Command: show startup-config netflow
!Time: Tue Feb  2 22:43:13 2010
!Startup config saved at: Thu Jan 21 08:39:42 2010

version 5.0(2)
feature netflow

flow exporter new_flow_1
  version 5
flow exporter new_flow_2
  version 9
```



```
flow exporter test
  version 9
flow exporter Custom-Flow-Exporter-1
  version 9
  option exporter-stats timeout 1200

switch#
```

**Related Commands**

Command	Description
<b>show running-config netflow</b>	Displays information about the NetFlow configuration that is currently running on the switch.

# show startup-config ntp

To display the Network Time Protocol (NTP) startup configuration, use the **show startup-config ntp** command.

**show startup-config ntp [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays all NTP startup configurations.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display the NTP startup configuration:
-----------------	--

```
switch(config)# show startup-config ntp

!Command: show startup-config ntp
!Time: Tue Feb  2 22:45:37 2010
!Startup config saved at: Thu Jan 21 08:39:42 2010

version 5.0(2)
ntp server 192.0.2.10 use-vrf Red
ntp peer 2001:db8::4101
ntp authenticate
ntp authentication-key 42 md5 dJmhwKzd 7
ntp trusted-key 42
ntp logging
ntp access-group peer NT_GLOBAL

switch(config)#
```

Related Commands	Command	Description
	<b>show ntp source-interface</b>	Displays information about the NTP source interface.
	<b>show running-config ntp</b>	Displays information about the NTP configuration that is currently running on the switch.

# show startup-config snmp

To display the startup Simple Network Management Protocol (SNMP) configuration of a system, use the **show startup-config snmp** command.

**show startup-config snmp [all]**

<b>Syntax Description</b>	<b>all</b> (Optional) Displays the startup SNMP configuration with defaults.				
<b>Defaults</b>	None				
<b>Command Modes</b>	Any command mode				
<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.1(2)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.1(2)	This command was introduced.
Release	Modification				
4.1(2)	This command was introduced.				
<b>Usage Guidelines</b>	This command does not require a license.				

**Examples**

This example shows how to display the startup SNMP configuration of the system:

```
switch(config)# show startup-config snmp

!Command: show startup-config snmp all
!Time: Tue Feb  2 22:46:33 2010
!Startup config saved at: Thu Jan 21 08:39:42 2010

version 5.0(2)
snmp-server aaa-user cache-timeout 3600
snmp-server protocol enable
no snmp-server globalEnforcePriv
snmp-server tcp-session auth
snmp-server user admin network-admin auth md5 0x1dc65f45a9d8e41dbccd76380946d6c3
  priv 0x1dc65f45a9d8e41dbccd76380946d6c3 localizedkey
snmp-server enable traps ospf rate-limit 10 7
snmp-server enable traps ospf foo rate-limit 10 7
no snmp-server enable traps bridge topologychange
no snmp-server enable traps bridge newroot
no snmp-server enable traps stpx inconsistency
no snmp-server enable traps stpx loop-inconsistency
no snmp-server enable traps stpx root-inconsistency

switch(config-port-monitor)#
```

**Related Commands**

Command	Description
<b>show running-config snmp</b>	Displays the running SNMP configuration.
<b>show port-monitor active</b>	Displays active port-monitor policies.

# show system cores

To display the core filename, use the **show system cores** command.

**show system cores**

---

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

---

**Defaults** Displays information for all features.

---

**Command Modes** Any command mode

---

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

---

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

---



---

**Usage Guidelines** Use the **system cores** command to configure the system core filename.  
This command does not require a license.

---

**Examples** This example shows how to display destination information for the system core files:

```
switch# show system cores
Cores are transferred to slot0:
```

---

Related Commands	Command	Description
	<b>system cores</b>	Configures the system core filename.

---

# show system error-id

To display the destination information for core files, use the **show system error-id** command.

```
show system error-id {error-number | list}
```

Syntax Description	<i>error-id</i>	Error number. The range is from 0x0 to 0xffffffff.
	<b>list</b>	Displays brief information for all the system error messages.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

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

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

**Examples** This example shows how to display detailed information for an error message:

```
switch# show system error-id 0x1
```

```
Error Facility: (null)
Error Description: not enough memory
```

This example shows how to display brief information for all the error messages:

```
switch# show system error-id list
```

```
Common errors:
 0x00000000 (SYSERR_SUCCESS): "success".
 0x00000001 (SYSERR_NOMEM): "not enough memory".
 0x00000002 (SYSERR_PSS_ERROR): "error while accessing PSS".
 0x00000003 (SYSERR_CMI_NO_RESPONSE_PAYLOAD): "no cmi response payload".
 0x00000004 (SYSERR_CMI_NULL_RECEIVE_BUF): "null cmi receive buffer".
 0x00000005 (SYSERR_MGMT_ERROR): "unknown error".
 0x00000006 (SYSERR_MGMT_NO_ENTRY): "entry not present".
 0x00000007 (SYSERR_MGMT_NO_OBJECT): "object not present".
...
```

# show system internal dir

To list all the files in a specific directory path along with the file sizes, use the **show system internal dir** command.

**show system internal dir** *directory-path*

<b>Syntax Description</b>	<i>directory-path</i>	The complete directory path.
---------------------------	-----------------------	------------------------------

<b>Defaults</b>	None.
-----------------	-------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin vdc-admin network-operator vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.2(4)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display all the files in a specific directory path along with the file sizes:
-----------------	---

```
switch# show system internal dir /etc
./ 2660
../ 1020
dcos-xinetd.pid 10
shadow 1394
passwd 1817
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show system internal file</b>	Lists the contents of a specific file.



# show system internal file

To list the contents of a file, use the **show system internal file** command.

**show system internal file** *file-name*

<b>Syntax Description</b>	<i>file-name</i>	The complete file path.
---------------------------	------------------	-------------------------

<b>Defaults</b>	None.
-----------------	-------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin vdc-admin network-operator vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.2(4)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to display all the files in a specific directory path along with the file sizes:

```
switch# show system internal file /bootflash/poap_debugs_7191.txt
<Wed Apr 1 01:23:02 2015> ../feature/poap/server/poap_main.c:main: getrlimit re
turns, soft:4294967295, hard: 4294967295.
poap_initialize(315): timer library initialization successful
poap_initialize(334): poap_db_initialize done
poap_mts_queue_initialize(147): mts bind for poap_q_mts(10) successful
poap_mts_queue_initialize(182): registered MTS_OPC_SDWRAP_DEBUG_DUMP(1530) with
poap_q_mts
poap_mts_queue_initialize(182): registered MTS_OPC_SYSLOG_FACILITY_OPR(185) with
poap_q_mts
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show system internal dir</b>	List all the files in a specific directory path along with the file sizes.

# show system internal scale-parameters

To display scale parameters, use the show system internal scale-parameters command.

**show system internal scale-parameters** [**configured** | **supported** | **violated** [**summary** | **vdc**]]

Syntax Description	Parameter	Description
	<b>configured</b>	Displays the configured scale limits.
	<b>supported</b>	Displays the scale limits supported in the current software version.
	<b>violated</b>	Displays the currently violated scale limits.
	<b>summary</b>	Displays the summary of scale limits for the switch.
	<b>vdc</b>	Displays scale limits for a specific VDC.

**Defaults** None.

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

Command History	Release	Modification
	7.2(1)D1(1)	This command was introduced.

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

**Examples** This example show how to display scale limits for a switch:



**Note**

If the configured scale limit exceeds the maximum permissible limit, then it displays a "Y" in the violated column for the specific scale parameter.

```
switch# show system internal scale-parameters
Scale Parameters for entire switch:
Parameter                               Supported   Configured  Violated(Y/N)
-----
FEX server interfaces                   3072       0           N
F1 HW entries                           256000     0           N
vPCs                                    744        0           N
Fabric Extenders(FEXs)                  64         0           N
Edge-ports                              384        1           N
port-channels                           744        0           N
```

IS-IS adjacencies	256	0	N
BFD-sessions	2000	0	N
L2-mroutes	32000	5001	N
M2 HW entries	128000	0	N
Core-ports	256	0	N
M1 HW entries	128000	0	N
FabricPath Switch-ids	256	0	N
VLANs	4000	5001	Y
FabricPath Topologies	8	0	N
F2/F2e HW entries	192000	0	N

## Scale Parameters for VDC: switch

Parameter	Supported	Configured	Violated(Y/N)
FEX server interfaces	3072	0	N
F1 HW entries(module 3)	256000	0	N
vPCs	744	0	N
Fabric Extenders(FEXs)	64	0	N
Edge-ports	384	1	N
port-channels	744	0	N
MSTP	64	0	N
IS-IS adjacencies	256	0	N
BFD-sessions	2000	0	N
L2-mroutes	32000	3000	N
M2 HW entries(module 4)	128000	3000	N
Core-ports	256	0	N
M1 HW entries	128000	0	N
FabricPath Switch-ids	256	0	N
VLANs	4000	3000	N
FabricPath Topologies	8	0	N
F2/F2e HW entries	192000	0	N

## Scale Parameters for VDC: v2

Parameter	Supported	Configured	Violated(Y/N)
FEX server interfaces	3072	0	N
F1 HW entries(module 3)	256000	0	N
vPCs	744	0	N
Fabric Extenders(FEXs)	64	0	N
Edge-ports	384	0	N
port-channels	744	0	N
MSTP	64	0	N
IS-IS adjacencies	256	0	N
BFD-sessions	2000	0	N
L2-mroutes	32000	1	N
M2 HW entries(module 4)	128000	0	N
Core-ports	256	0	N
M1 HW entries	128000	0	N
FabricPath Switch-ids	256	0	N
VLANs	4000	1	N
FabricPath Topologies	8	0	N
F2/F2e HW entries	192000	0	N

This example shows how to display a summary of the currently violated scale limits on a switch:

```
switch# show system internal scale-parameters violated summary
```

Scale Parameters for entire switch:

Parameter	Supported	Configured	Violated(Y/N)
VLANs	4000	5001	Y

■ show system internal scale-parameters

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>system scale-limit monitor</b>	Enables scale limit monitoring on a switch.

---

# show system memory-status

To display the memory status information, use the **show system memory-status** command.

**show system memory-status**

---

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

---

**Defaults** Displays information for all features.

---

**Command Modes** Any command mode

---

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

---

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

---

---

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

---

**Examples** This example shows how to display the memory status information:

```
switch# show system memory-status
MemStatus: OK
```

# show system mode

To display the current system mode, use the **show system mode** command. Starting with Cisco NX-OS Release 7.3(0)D1(1), you can use the **show system mode** command to also display the current state of the maintenance mode timer when the switch is in maintenance mode

```
show system mode
```

---

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

---

**Defaults** None

---

**Command Modes** Any command mode

---

Command History	Release	Modification
	7.3(0)D1(1)	Supports display of current state of the maintenance mode timer when the switch is in maintenance mode.
	7.2.0	This command was introduced.

---



---

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

---

**Examples** This example shows how to display the current system mode:

```
switch# show system mode
System Mode : Normal
```

This example shows how to display the current system mode and the state of the maintenance mode timer when the switch is in maintenance mode:

```
switch# show system mode
System Mode: Maintenance
Maintenance Mode Timer: 24 minutes 55 seconds remaining
```

This example shows that the switch is in maintenance mode and that the maintenance mode timer is not running:

```
switch# show system mode
System Mode: Maintenance
Maintenance Mode Timer: not running
```

---

Related Commands

Command	Description
<b>show run mmode</b>	Displays the currently running maintenance profile configuration on a switch.
<b>system mode maintenance always-use-custom-profile</b>	Applies the existing custom maintenance-mode profile and prevents creation of auto-generated maintenance-mode profile.
<b>system mode maintenance on-reload reset-reason</b>	Boots the switch into maintenance-mode automatically in the event of a specified system crash.
<b>system mode maintenance shutdown</b>	Shuts down all protocols and interfaces except the management interface (by using the <b>shutdown</b> command and not the default <b>isolate</b> command).
<b>system mode maintenance timeout</b>	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

# show system pss shrink status

To display the last Persistent Storage Service (PSS) shrink status, use the **show system pss shrink status** command.

**show system pss shrink status**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the last PSS shrink status:

```
switch(config)# show system pss shrink status
Last pss shrink started on: Tue May 12 08:08:30 2009
switch(config)#
```

Related Commands	Command	Description
	<b>show system pss shrink status details</b>	Displays the last PSS shrink status details.



# show system pss shrink status details

To display details of the last Persistent Storage Service (PSS) shrink status details, use the **show system pss shrink status details** command.

**show system pss shrink status details**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display details of the last PSS shrink status:

```
switch(config)# show system pss shrink status details
Last pss shrink started on: Tue May 12 08:08:30 2009

VDC 1:
Service "aaa" in vdc 1: pss shrink completed successfully
Service "cert_enroll" in vdc 1: pss shrink completed successfully
Service "ExceptionLog" in vdc 1: pss shrink completed successfully
Service "psshelper_gsvc" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "platform" in vdc 1: pss shrink completed successfully
Service "R2D2_usd" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "radius" in vdc 1: pss shrink completed successfully
Service "securityd" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "tacacs" in vdc 1: pss shrink completed successfully
Service "eigrp" in vdc 1: pss shrink request not sent
Service "isis" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "isis_dce" in vdc 1: pss shrink request not sent
Service "isis_otv" in vdc 1: pss shrink request not sent
Service "ospf" in vdc 1: pss shrink request not sent
Service "ospfv3" in vdc 1: pss shrink request not sent
Service "rip" in vdc 1: pss shrink request not sent
Service "eigrp" in vdc 1: pss shrink request not sent
```

## show system pss shrink status details

```

Service "isis" in vdc 1: pss shrink request not sent
Service "isis_dce" in vdc 1: pss shrink request not sent
Service "ospf" in vdc 1: pss shrink request not sent
Service "ospfv3" in vdc 1: pss shrink request not sent
Service "rip" in vdc 1: pss shrink request not sent
Service "eigrp" in vdc 1: pss shrink request not sent
Service "isis" in vdc 1: pss shrink request not sent
Service "isis_dce" in vdc 1: pss shrink request not sent
Service "ospf" in vdc 1: pss shrink request not sent
Service "ospfv3" in vdc 1: pss shrink request not sent
Service "rip" in vdc 1: pss shrink request not sent
Service "eigrp" in vdc 1: pss shrink request not sent
Service "isis" in vdc 1: pss shrink request not sent
Service "isis_dce" in vdc 1: pss shrink request not sent
Service "ospf" in vdc 1: pss shrink request not sent
Service "ospfv3" in vdc 1: pss shrink request not sent
Service "rip" in vdc 1: pss shrink request not sent
Service "acllog" in vdc 1: pss shrink completed successfully
Service "aclmgr" in vdc 1: pss shrink completed successfully
Service "adjmgr" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "amt" in vdc 1: pss shrink request not sent
Service "arbiter" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "arp" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "ascii-cfg" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "babycaesar" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "bgp" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "bios_daemon" in vdc 1: pss shrink request not sent
Service "bootup_test" in vdc 1: pss shrink request not sent
Service "bootvar" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "callhome" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "capability" in vdc 1: pss shrink completed successfully
Service "cardclient" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "cdp" in vdc 1: pss shrink completed successfully
Service "cfs" in vdc 1: pss shrink completed successfully
Service "clis" in vdc 1: pss shrink not needed (defaultcb invoked)
Service "cmpproxy" in vdc 1: pss shrink completed successfully
Service "confcheck" in vdc 1: pss shrink completed successfully
--More--

```

### Related Commands

Command	Description
<b>show system pss shrink status</b>	Displays the last PSS shrink status.

# show system reset-reason

To display the reset-reason history for the modules on the device, use the **show system reset-reason** command.

**show system reset-reason** [**module** *slot* | **xbar** *xbar-number*]

Syntax Description	Parameter	Description
	<b>module</b> <i>slot</i>	(Optional) Displays the restart reason for an I/O module or supervisor module.
	<b>xbar</b> <i>xbar-number</i>	(Optional) Displays the restart reason for the fabric module.

**Defaults** Displays the reset reasons for the supervisor modules.

**Command Modes** Any command mode

**Supported User Roles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** You can use this command only in the default virtual device context (VDC).  
This command does not require a license.

**Examples** This example shows how to display the reset-reason history for the supervisor modules:

```
switch# show system reset-reason
----- reset reason for Supervisor-module 6 (from Supervisor in slot 6) ---
1) At 11151 usecs after Fri May 30 14:40:50 2008
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 4.0(2)
2) At 171083 usecs after Wed May 28 11:40:49 2008
   Reason: Reset Requested by CLI command reload
   Service:
   Version: 4.0(2)
----- reset reason for Supervisor-module 5 (from Supervisor in slot 6) ---
1) No time
   Reason: Unknown
   Service:
   Version:
2) No time
```

## ■ show system reset-reason

```
Reason: Unknown  
Service:  
Version:
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear system reset-reason</b>	Clears the reset reason history for the device.

---

# show system redundancy

To display the system redundancy status, use the **show system redundancy** command.

**show system redundancy [ha] status**

<b>Syntax Description</b>	<b>ha</b> (Optional) Displays the virtual device context (VDC) redundancy status.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator
---------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to display the system redundancy status:
-----------------	---

```
switch# show system redundancy status
Redundancy mode
-----
      administrative:  HA
      operational:    None

This supervisor (sup-1)
-----
      Redundancy state:  Active
      Supervisor state:  Active
      Internal state:    Active with no standby

Other supervisor (sup-2)
-----
      Redundancy state:  Not present
switch#
```

This example shows how to display the virtual device context (VDC) redundancy status:

```
switch# show system redundancy ha status
VDC No   This supervisor           Other supervisor
-----   -
```

## ■ show system redundancy

```
vdc 1    Active with no standby    N/A
vdc 2    Active with no standby    N/A
vdc 3    Active with no standby    N/A
vdc 4    N/A                      N/A
switch#
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>system switchover</b>	Switches over to the standby supervisor.

---

# show system resources

To display the system resources, use the **show system resources** command.

**show system resources**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the system resources:

```
switch(config)# show system resources
Load average:  1 minute: 0.00   5 minutes: 0.00   15 minutes: 0.0
Processes   :  520 total, 1 running
CPU states  :  0.0% user,   0.5% kernel,  99.5% idle
Memory usage: 4135616K total,  1642556K used,  2493060K free
              1188K buffers,  731988K cache
switch(config)#
```

Related Commands	Command	Description
	<b>show processes cpu</b>	Displays the CPU utilization information for processes on the device.

# show system standby manual-boot

To display the status of the system standby manual boot option, use the **show system standby manual-boot** command.

**show system standby manual-boot**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display the status of the system standby manual boot option:

```
switch(config)# show system standby manual-boot
system standby manual-boot option is enabled
switch(config)#
```

Related Commands	Command	Description
	<b>system hap-reset</b>	Enables the Supervisor Reset HA policy.



# show system uptime

To display the amount of time since the last system upload, use the **show system uptime** command.

## **show system uptime**

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

**Defaults** Displays information for all features.

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
vdc-admin  
network-operator  
vdc-operator

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

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

**Examples** This example shows how to display the amount of time since the last system reload:

```
switch# show system uptime
System start time:      Fri May 30 14:46:25 2008
System uptime:         16 days, 23 hours, 9 minutes, 22 seconds
Kernel uptime:         16 days, 23 hours, 13 minutes, 29 seconds
Active supervisor uptime: 16 days, 23 hours, 9 minutes, 22 seconds
```

# show tech-support all binary

To collect logs from across the entire device in binary format, including virtual device contexts (VDCs) and linecards, use the **show tech-support all binary** command.

```
show tech-support all binary { bootflash: | logflash: | slot0: }
```

## Syntax Description

<b>bootflash:</b>	Specifies bootflash as the destination file system used to save the binary output.
<b>logflash:</b>	Specifies logflash as the destination file system used to save the binary output.
<b>slot0:</b>	Specifies slot0 as the destination file system used to save the binary output.

## Defaults

None

## Command Modes

Any command mode

## Supported User Roles

network-admin  
network-operator  
vdc-admin  
vdc-operator

## Command History

Release	Modification
6.2(2)	This command was introduced.

## Usage Guidelines

Binary tech support is a log-collecting framework that collects logs internally from all Cisco NX-OS processes that are running on the device. The **show tech-support all binary** command collects logs from across the entire device, including VDCs, and line cards. The logs are saved under one tarball that can be easily transferred for later analysis.

Binary tech support can either be parsed within the device or moved to an external log server where it can be parsed offline. The tool that is used to parse the logs is called DeBlogger. If a line card fails during the log collection, binary tech support continues to collect logs from all remaining line cards and VDCs.



### Note

The output filename is automatically generated and cannot be chosen.

This command does not require a license.

## Examples

This example shows how to collect logs from across the entire device:

```
switch(config)# show tech-support all binary bootflash:
```

```

Temporary Storage Space Available: 1345 MB
Destination Storage Space Available: 229 MB
Waiting for all Modules to dump 'Binary Tech Support'...
Response from module: 7 is: 0x0(SUCCESS/Success)
Response from module: 4 is: 0x0(SUCCESS/Success)
Response from module: 9 is: 0x0(SUCCESS/Success)
Response from module: 5 is: 0x0(SUCCESS/Success)
Response from module: 6 is: 0x0(SUCCESS/Success)
-----
Please find the output here:
bootflash:binary_show_tech_all_06_12_2013_14_26_05HRS.tar
-----
    
```

**Related Commands**

Command	Description
<b>bloggerd parse</b> <b>log-buffer</b>	Parses logs from binary to ASCII format.

# show tech-support ascii-cfg

To display detailed information about the checkpoint feature, use the **show tech-support ascii-cfg** command.

## show tech-support ascii-cfg

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to show the detailed information about the checkpoint feature:

```
switch# show tech-support ascii-cfg
`show checkpoint summary`
-----
Name                UserName                Created at
-----
stable              admin                   Tue May 27 13:19:24 2008
`show checkpoint`
-----
Name: stable
version 4.0(2)
power redundancy-mode combined force
license grace-period
feature vrp
feature tacacs+
feature ospf
feature pim
feature pim6
feature msdp
feature eigrp
feature rip
feature isis
```

```
feature pbr
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show checkpoint</b>	Displays the contents of the checkpoint file.

# show tech-support cfs

To display information about the Cisco Fabric Services (CFS) configuration required by technical support, use the **show tech-support cfs** command.

```
show tech-support cfs {commands} | [name application_name {commands}]}
```

Syntax Description	commands	Displays all related CFS commands for use when working with technical support on a CFS issue.
	name application_name	(Optional) Displays information about the CFS configuration required by technical support for a specific application.

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.1(2)	This command was introduced.

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

**Examples** This example shows how to display information about the CFS configuration required by technical support:

```
switch# show tech-support cfs
`show cfs application`
```

```
-----
Application    Enabled    Scope
-----
ntp            No        Physical-fc-ip
stp            Yes       Physical-eth
vpc            Yes       Physical-eth
igmp           Yes       Physical-eth
l2fm           Yes       Physical-eth
role           No        Physical-fc-ip
radius         No        Physical-fc-ip
callhome       Yes       Physical-fc-ip
```

```

Total number of entries = 8

`show cfs lock`
`show cfs peers`

Physical Fabric
-----
Switch WWN                IP Address
-----
20:00:00:22:55:79:a4:c1 172.28.230.85          [Local]
                        switch

Total number of entries = 1

`show cfs status`
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
Distribution over Ethernet : Disabled`show cfs internal event-history errors`
Mon Dec 22 12:24:42 2008 :
Sending over network failed, retval ffffffff, errno 113 [No route to host]
Msg ID: [6e:00:00:00:c0:e0:ff:bf:0:1]
vsan: 4097, IP addr: 0.0.0.0

Total number of entries = 8

```

**Related Commands**

Command	Description
<b>show <i>application_name</i> session status</b>	Displays the CFS configuration session status for the application, including the last action, the result, and the reason if there was a failure.
<b>show cfs internal</b>	Displays information internal to CFS including memory statistics, event history, and so on.
<b>show cfs lock</b>	Displays all active CFS fabric locks.
<b>show cfs merge status <i>name</i></b>	Displays the merge status for a given CFS application.
<b>show cfs peers</b>	Displays all the CFS peers in the physical fabric.
<b>show cfs regions</b>	Displays all the CFS applications with peers and region information.
<b>show cfs static</b>	Displays all CFS static peers with their status.
<b>show cfs status</b>	Displays the status of CFS distribution on the device as well as IP distribution information.

# show tech-support mmode

To display information for maintenance profile troubleshooting, use the **show tech-support mmode** command.

## show tech-support mmode

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

**Defaults** None

**Command Modes** Privileged EXEC

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

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

**Examples** This example shows how to display information for maintenance profile troubleshooting:

```
switch# show tech-support mmode
`show system mode`
System Mode: Normal
`show maintenance profile`
[Normal Mode]
router bgp 100
  no isolate

[Maintenance Mode]
router bgp 100
  isolate

`show maintenance on-reload reset-reasons`
Reset reasons for on-reload maintenance mode:
-----
(not configured)

bitmap = 0x0
`show maintenance timeout`
Maintenance mode timeout value: 0 minutes
`show system internal mmode mem-stats`
```



Num blocks	User size	Total size	Library
16	560	800	mmode
265	51818	55824	ld-2.8.so
1	20	32	libdl-2.8.so
1	38	56	libpthread-2.8.so
12	2860	3056	libsvifdb.so.0.0.0

**Related Commands**

Command	Description
<b>system mode maintenance always-use-custom-profile</b>	Applies the existing custom maintenance-mode profile and prevents creation of auto-generated maintenance-mode profile.
<b>system mode maintenance on-reload reset-reason</b>	Boots the switch into maintenance-mode automatically in the event of a specified system crash.
<b>system mode maintenance shutdown</b>	Shuts down all protocols and interfaces except the management interface (by using the <b>shutdown</b> command and not the default <b>isolate</b> command).
<b>system mode maintenance timeout</b>	Configures the maintenance window timer to keep the switch in maintenance mode for a specified number of minutes.

# show tech-support session-mgr

To display detailed information about the session manager, which controls configuration sessions, use the **show tech-support session-mgr** command.

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** Use the **show tech-support session-mgr** command to gather information about the session manager for troubleshooting purposes. This command displays detailed information about the session manager. The output should be saved to a file and included in any support requests for the session manager.

This command does not require a license.

**Examples** This example shows how to save the output of the **show tech-support session-mgr** command to a file:

```
switch# show tech-support session-mgr > bootflash:output
```

Related Commands	Command	Description
	<b>show configuration session</b>	Displays information about the configuration sessions.

# show tech-support snmp

To display detailed technical support information for Simple Network Management Protocol (SNMP), use the **show tech-support snmp** command.

**show tech-support snmp**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** Use the **show tech-support snmp** command to gather information about SNMP for troubleshooting purposes. This command displays detailed information about SNMP. The output should be saved to a file and included in any support requests for SNMP.

This command does not require a license.

**Examples** This example shows how to save the output of the **show tech-support snmp** command to a file:

```
switch# show tech-support snmp > bootflash:output
```

Related Commands	Command	Description
	snmp-server community	Configures SNMP community strings.

# show tech-support slowdrain

To display detailed technical support information for the slow drain feature, use the **show tech-support slowdrain** command.

**show tech-support slowdrain**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** Use the **show tech-support slowdrain** command to gather information about the slow drain feature for troubleshooting purposes. This command displays detailed information about slow drain. The output should be saved to a file and included in any support requests for slow drain.

This command does not require a license.

**Examples** This example shows how to save the output of the **show tech-support slowdrain** command to a file:

```
switch# show tech-support slowdrain > bootflash:output
```

Related Commands	Command	Description
	<b>system default interface congestion timeout</b> <i>milliseconds</i> <b>mode</b> {core   edge}	Configures slow drain congestion timeout value for Cisco NX-OS Release 8.1(1) and earlier releases.
	<b>system default interface pause timeout</b> <i>milliseconds</i> <b>mode</b> {core   edge}	Configures slow drain pause timeout value for Cisco NX-OS Release 8.1(1) and earlier releases.

Command	Description
<b>system timeout fcoe congestion-drop</b> { <i>milliseconds</i>   <b>default</b> } <b>mode</b> { <b>core</b>   <b>edge</b> }	Configures slow drain congestion timeout value for Cisco NX-OS Release 8.2(1) and earlier releases.
<b>system timeout fcoe pause-drop</b> { <i>milliseconds</i>   <b>default</b> } <b>mode</b> { <b>core</b>   <b>edge</b> }	Configures slow drain pause timeout value for Cisco NX-OS Release 8.2(1) and earlier releases.

# show xml server status

To display information about the status of the XML server, use the **show xml server status** command.

## show xml server status

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to display information about the status of the XML server:

```
switch(config)# show xml server status
operational status is enabled
maximum session configured is 8
switch(config)#
```



# System Message Logging Facilities

Table 1-1 lists the facilities that you can use in system message logging configuration.

**Table 1-1** System Message Logging Facilities

Facility	Description
aaa	AAA manager
aclog	ACL log manager
aclmgr	ACL manager
adjmgr	Adjacency manager
all	Keyword that represents all facilities
amt	AMT manager
arbiter	Arbiter manager
arp	ARP manager
ascii-cfg	ASCII configuration
auth	Authorization system
authpriv	Private authorization system
bfd_app	Bidirectional Forwarding Detection (BFD)
bgp	BGP manager
bootvar	Bootvar
callhome	Call home manager
capability	MIG utilities daemon
cdp	CDP manager
cfs	Cisco Fabric Services (CFS)
clis	CLIS manager
cmpproxy	CMP proxy manager
copp	CoPP manager
core	Core daemon
cron	Cron and at scheduling service
cts	CTS manager
daemon	System daemons

**Table 1-1** System Message Logging Facilities (continued)

Facility	Description
dcbx	Discovery protocol manager
device_test	GOLD Device Test
dhcp_snoop	DHCP snooping
diagclient	GOLD diagnostic client manager
diagmgr	GOLD diagnostic manager
dot1x	802.1X manager
eigrp	EIGRP manager
eltm	ELTM manager
eou	EOU manager
ethdstats	Delta statistics manager
ethpm	Ethernet PM manager
evmc	EVMC manager
evms	EVMS manager
feature-mgr	Feature manager
fs-daemon	Fs daemon
ftp	File transfer system
glbp	GLBP manager
hsrp_engine	HSRP manager
im	IM manager
interface-vlan	VLAN interfaces (SVI) manager
ip igmp	IGMP manager
ip msdp	MSDP manager
ip pim	IPv4 PIM manager
ipconf	IP configuration manager
ipqos	IP QoS manager
ipv6 icmp	IPv6 ICMP
ipv6 pim	IPv6 PIM
isis	IS-IS manager
kernel	OS kernel
keystore	Keystore manager
l2fm	L2 FM manager
l3vm	L3 VM manager
lACP	LACP manager
license	Licensing manager
lisp	LISP manager
local0	Local use daemon



**Table 1-1** System Message Logging Facilities (continued)

Facility	Description
local1	Local use daemon
local2	Local use daemon
local3	Local use daemon
local4	Local use daemon
local5	Local use daemon
local6	Local use daemon
local7	Local use daemon
lpr	Line printer system
mail	Mail system
mfdm	MFDM manager
module	Module manager
monitor	Ethernet SPAN manager
mvsh	MVSH manager
netstack	IP/IPv6 network stack
news	USENET news
nfm	NFM manager
ntp	NTP manager
ospf	OSPF manager
ospfv3	OSPF manager
pfstat	PFSTAT manager
pixm	PIXM manager
platform	Platform manager
pltfm_config	PLTFM configuration manager
plugin	Plug-in manager
port-security	Port security manager
port_lb	Diagnostic port loopback test manager
private-vlan	Private VLAN manager
qengine	Q engine manager
radius	RADIUS manager
res_mgr	Resource manager
rip	RIP manager
routing ipv6 multicast	IP, IPv4 multicast routing manager
routing multicast	IPv6 multicast routing manager
rpm	RPM manager
sal	SAL manager
scheduler	Scheduler

**Table 1-1** System Message Logging Facilities (continued)

Facility	Description
security	Security manager
session-mgr	Session manager
smm	Shared memory manager
snmpd	SNMP daemon
spanning-tree	STP manager
syslog	Internal syslog manager
sysmgr	System manager
tacacs+	TACACS+ manager
track	Track manager
tunnel	Tunnel manager
u2	U2 manager
u6rib	U6RIB manager
udld	UDLD manager
ufdm	UFDM manager
urib	URIB manager
user	User process
uucp	UNIX-to-UNIX copy system
vdc_mgr	VDC manager
vlan_mgr	VLAN manager
vmm	VMM manager
vrrp_cfg	VRRP engine and configuration manager
vshd	VSHD manager
xbar_client	XBAR client manager
xml server	XML agent

## Debug Messages

Debug messages logged by enabling **debug** CLI are not syslog messages, these messages are not sent to any syslog destinations.



# T Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter T.

# 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	
<i>tag</i>	Tag name. The tag name can be any 29 alphanumeric characters.
<b>and</b>	(Optional) Specifies to use boolean and logic
<b>andnot</b>	(Optional) Specifies to use boolean andnot logic
<b>or</b>	(Optional) Specifies to use boolean or logic
<b>happens</b>	Specifies the number of occurrences before raising the event.
<b>in</b>	Specifies the number of occurrences must occur within this time period.
<i>occurs</i>	Numbers of times that the event occurs. The range is from 1 to 4294967295.
<i>seconds</i>	Amount of time, in seconds, that the next event occurs. The range is from 0 to 4294967295 seconds.

Defaults	
	None

Command Modes	
	(config-applet)

SupportedUserRoles	
	network-admin vdc-admin

Command History	Release	Modification
	5.2(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 e 3/1
```

Related Commands	Command	Description
	<b>show flow exporter</b>	Displays information about NetFlow exporters.



# template data timeout

To configure the template data timeout parameter for the NetFlow exporter, use the **template data timeout** command. To remove the template data timeout parameter, use the **no** form of this command.

**template data timeout** *time*

**no template data timeout** [*time*]

<b>Syntax Description</b>	<i>time</i> (Optional) Time in seconds. The range is from 1 to 86400.				
<b>Defaults</b>	None				
<b>Command Modes</b>	NetFlow exporter version 9 configuration (config-flow-exporter-version-9)				
<b>SupportedUserRoles</b>	network-admin vdc-admin				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
<b>Usage Guidelines</b>	This command does not require a license.				
<b>Examples</b>	<p>This example shows how to configure the template data timeout parameter:</p> <pre>switch(config)# flow exporter Netflow-Exporter-1 switch(config-flow-exporter)# version 9 switch(config-flow-exporter-version-9)# template data timeout 120</pre> <p>This example shows how to remove the template data timeout parameter configuration:</p> <pre>switch(config-flow-exporter)# version 9 switch(config-flow-exporter-version-9)# no template data timeout 120</pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show flow exporter</b></td> <td>Displays information about NetFlow exporters.</td> </tr> </tbody> </table>	Command	Description	<b>show flow exporter</b>	Displays information about NetFlow exporters.
Command	Description				
<b>show flow exporter</b>	Displays information about NetFlow exporters.				

# terminal event-manager bypass

To allow the CLI commands that match an Embedded Event Manager (EEM) policy to continue to run, use the **terminal event-manager bypass** command. To prevent such commands from running, use the **no** form of this command.

**terminal event-manager bypass**

**terminal no event-manager bypass**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	4.2(1)	This command was introduced.

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

**Examples** This example shows how to allow the CLI commands that match an EEM policy to continue to run:

```
switch# terminal event-manager bypass
switch#
```

This example shows how to prevent the CLI commands that match an EEM policy from running:

```
switch# terminal no event-manager bypass
switch#
```

Related Commands	Command	Description
	<b>event manager policy</b>	Registers an Embedded Event Manager (EEM) policy with the EEM.

# test watchdog

To test the watchdog feature, use the **test watchdog** command.

**test watchdog**

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

**Defaults** None

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

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

**Examples** This example shows how to test the watchdog feature:

```
switch(config)# test watchdog
Warning: This command will reboot the system if watchdog is functioning properly
.
Do you wish to proceed anyway? (y/n)
```

Related Commands	Command	Description
	<b>system watchdog</b>	Enables the watchdog feature.
	<b>system no watchdog</b>	Disables the watchdog feature.



# transport email mail-server

To configure up to five SMTP servers as the domain name server (DNS) names, IPv4 addresses, or IPv6 addresses for Call home, use the **transport email mail-server** command.

```
transport email mail-server ip-address [port port-number] [priority priority-number] [use-vrf vrf-name]
```

Syntax Description	
<i>ip-address</i>	Domain name server (DNS) name, IPv4 address, or IPv6 address.
<b>port</b> <i>port-number</i>	(Optional) Specifies the port number. The range is from 1 to 65535. The default port number is 25.
<b>priority</b> <i>priority-number</i>	(Optional) Specifies the priority of the SMTP server. The range is from 1 to 100, with 1 being the highest priority and 100 the lowest. If you do not specify a priority, the default value of 50 is used.
<b>use-vrf</b> <i>vrf-name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) name.

**Defaults** None

**Command Modes** Call home configuration

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** You can configure up to five SMTP servers for Call home. The VRF specified in the **transport email mail-server** command is not used to send messages using HTTP. When CFS distribution is enabled, devices that run Release 4.2 or earlier releases accept only the **transport email smtp-server** command configurations while devices that run Release 5.0(1) or later releases accept both the **transport email smtp-server** and **transport email mail-server** command configurations.

When a device accepts both the **transport email smtp-server** and **transport email mail-server** commands, the **transport email smtp-server** command has a priority of 0, which is the highest. The server specified by this command is tried first followed by the servers specified by the **transport email mail-server** commands in order of priority.

This command does not require a license.

**Examples**

This example shows how to configure multiple SMTP servers for Call home messages:

```
switch(config)# callhome
switch(config-callhome)# transport email mail-server 192.0.2.1 port 33 priority 1 use-vrf
Red
switch(config-callhome)# transport email mail-server 192.0.2.10 priority 4
switch(config-callhome)# transport email mail-server 172.21.34.193
switch(config-callhome)# transport email smtp-server 10.1.1.174
switch(config-callhome)# transport email mail-server 64.72.101.213 priority 60
switch(config-callhome)# transport email from person@company.com
switch(config-callhome)# transport email reply-to person@company.com
switch(config-callhome)#
```

Based on the configuration above, the SMTP servers would be tried in this order:

10.1.1.174 (priority 0)

192.0.2.1 (priority 1)

172.21.34.193 (priority 50, which is the default)

64.72.101.213 (priority 60)

**Related Commands**

Command	Description
<b>transport http use-vrf</b>	Configures a VRF to send Call home messages using HTTP.
<b>transport email smtp-server</b>	Distributes the SMTP server configuration to devices that run Release 4.2 or earlier releases.

# transport http proxy enable

To enable Smart Call Home to send all HTTP messages through the HTTP proxy server, use the **transport http proxy enable** command.

**transport http proxy enable**

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

**Defaults** Disabled

**Command Modes** Call home configuration mode (config-callhome)

**SupportedUserRoles** network-admin  
vdc-admin

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

**Usage Guidelines** You can use this command only after the proxy server address has been configured. The virtual routing and forwarding (VRF) instance used for transporting messages through the proxy server is the same as that configured using the **transport http use-vrf** command. This command does not require a license.

**Examples** This example shows how to enable Smart Call Home to send all HTTP messages through the HTTP proxy server:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# transport http proxy server 192.0.2.1
switch(config-callhome)# transport http proxy enable
switch(config-callhome)#
```

Related Commands	Command	Description
	<b>transport http proxy server</b>	Configures the HTTP proxy server domain name server (DNS) name, IPv4 address, or IPv6 address.
	<b>show callhome transport</b>	Displays the transport-related configuration for Smart Call Home.

# transport http proxy server

To configure the HTTP proxy server domain name server (DNS) name, IPv4 address, or IPv6 address, use the **transport http proxy server** command.

```
transport http proxy server {ip-address | proxy-server-name} [port port-number]
```

Syntax Description	
<i>ip-address</i>	IPv4 or IPv6 address of the proxy server.
<i>proxy-server-name</i>	DNS name of the proxy server.
<b>port</b> <i>port-number</i>	(Optional) Specifies the port number. The range is from 1 to 65535. The default port number is 8080.

**Defaults** Disabled

**Command Modes** Call home configuration mode (config-callhome)

**Supported User Roles** network-admin  
vdc-admin

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

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

**Examples** This example shows how to configure the HTTP proxy server DNS name, IPv4 address, or IPv6 address:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# transport http proxy server http://www.yoursite.com port 5050
```

Related Commands	Command	Description
	<b>transport http proxy enable</b>	Enables Smart Call Home to send all HTTP messages through the HTTP proxy server.
	<b>show callhome transport</b>	Displays the transport-related configuration for Smart Call Home.

# transport http use-vrf

To configure the virtual routing and forwarding (VRF) instance used to send e-mail and other Call home messages over the Hypertext Transfer Protocol (HTTP), use the **transport http use-vrf** command.

**transport http use-vrf** *vrf-name*

<b>Syntax Description</b>	<i>vrf-name</i>	Virtual routing and forwarding (VRF) name. The name can any alphanumeric string up to 255 characters.
---------------------------	-----------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Call home configuration
----------------------	-------------------------

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	5.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to configure a VRF to send Call home messages using HTTP:

```
switch(config)# callhome
switch(config-callhome)# transport http use-vrf Blue
switch(config-callhome)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>transport email mail-server</b>	Configures multiple SMTP servers as the domain name server (DNS) names, IPv4 addresses, or IPv6 addresses for Call home.

# transport udp

To configure a NetFlow exporter to transport over UDP, use the **transport udp** command. To remove the transport configuration, use the **no** form of this command.

**transport udp** *port-number*

**no transport udp** [*port-number*]

<b>Syntax Description</b>	<i>port-number</i> (Optional) Destination UDP port number.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	NetFlow exporter configuration (config-flow-exporter)
----------------------	---

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

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

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to configure a NetFlow exporter to transport over UDP:
-----------------	---

```
switch(config)# flow exporter Netflow-Exporter-1
switch(config-flow-exporter)# transport udp 200
switch(config-flow-exporter)#
```

This example shows how to remove the UDP configuration:

```
switch(config-flow-exporter)# no transport udp 200
switch(config-flow-exporter)#
```

Related Commands	Command	Description
	<b>show flow exporter</b>	Displays information about NetFlow exporters.



# V Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter V.

# verify

To verify the commands in the configuration session, use the **verify** command.

**verify** [**verbose**]

<b>Syntax Description</b>	<b>verbose</b> (Optional) Verifies the current configuration session and displays more details on the results.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Session configuration
----------------------	-----------------------

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command does not require a license.
-------------------------	--

**Examples** This example shows how to verify a configuration session:

```
switch# configure session myACLs
switch(config-s)# verify
switch(config-s)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>commit</b>	Commits the commands in the configuration session.
	<b>abort</b>	Deletes the session and exists session configuration mode.



# version 5

To configure version 5 for the NetFlow exporter, use the **version 5** command. To remove the version 5 configuration, use the **no** form of this command

**version 5**

**no version 5**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

NetFlow exporter configuration (config-flow-exporter)

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

The default NetFlow exporter version is 5.

If you remove the version 5 configuration, the NetFlow exporter defaults to version 9.

This command does not require a license.

## Examples

This example shows how to configure the NetFlow exporter version to version 5:

```
switch(config)# flow exporter Netflow-Exporter-1
switch(config-flow-exporter)# version 5
switch(config-flow-exporter-version-5)#
```

This example shows how to remove the version 5 configuration, which causes the NetFlow exporter to default to version 9:

```
switch(config-flow-exporter-version-5)# no version 5
switch(config-flow-exporter)#
```

## Related Commands

Command	Description
<b>show flow exporter</b>	Displays information about NetFlow exporters.
<b>version 9</b>	Configures the NetFlow exporter to version 9.

# version 9

To specify the export version 9 and enter the export version configuration mode, use the **version 9** command.

**version 9**

**no version 9**

---

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

---

**Defaults** Flow exporters are not present in the configuration until you create them.

---

**Command Modes** Flow export configuration

---

**SupportedUserRoles** network-admin  
vdc-admin

---

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

---



---

**Usage Guidelines** Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.

Once you enter the flow exporter configuration mode, the prompt changes to the following:

```
switch(config-flow-exporter)#
```

Within the flow exporter configuration mode, you can enter the version 9 keywords. Once you enter the **version 9** keywords, the prompt changes to the following:

```
switch(config-flow-exporter-version-9)#
```

When entering the **no** form of this command, the *seconds* argument is optional.

This command does not require a license.

---

**Examples** This example shows how to specify the name of the flow exporter that is created or modified.

```
switch(config)# flow exporter flow-export-test
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)#
```

This example shows how to specify the version 9 exporter statistics option templates and data:

```
switch(config)# flow exporter flow-export-test
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# exporter-stats
```

This example shows how to specify the version 9 interface table option templates and data:

```
switch(config)# flow exporter flow-export-test
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# interface-table
```

This example shows how to specify the version 9 interface table option templates and data:

```
switch(config)# flow exporter flow-export-test
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# sampler-table
```

This example shows how to specify the option resend time in seconds:

```
switch(config)# flow exporter flow-export-test
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# timeout 32
```

This example shows how to specify the data template:

```
switch(config)# flow exporter flow-export-test
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# template data
```

#### Related Commands

Command	Description
<b>flow exporter</b>	Creates a flow exporter.
<b>flow monitor</b>	Creates a flow monitor.
<b>flow record</b>	Creates a flow record.
<b>sampler</b>	Creates a flow sampler.

# vrf

To configure a virtual routing and forwarding (VRF) instance for Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic forwarding in both the source and destination, use the **vrf** command.

```
vrf {vrf_name} | {[default | foo]}
```

## Syntax Description

<i>vrf_name</i>	Name of the VRF. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.
<b>default</b>	(Optional) Specifies the VRF name as the default.
<b>foo</b>	(Optional) Specifies the VRF name as foo.

## Defaults

None

## Command Modes

config-erspan-src  
config-erspan-dst

## Supported User Roles

network-admin  
network-operator

## Command History

Release	Modification
5.1(1)	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:

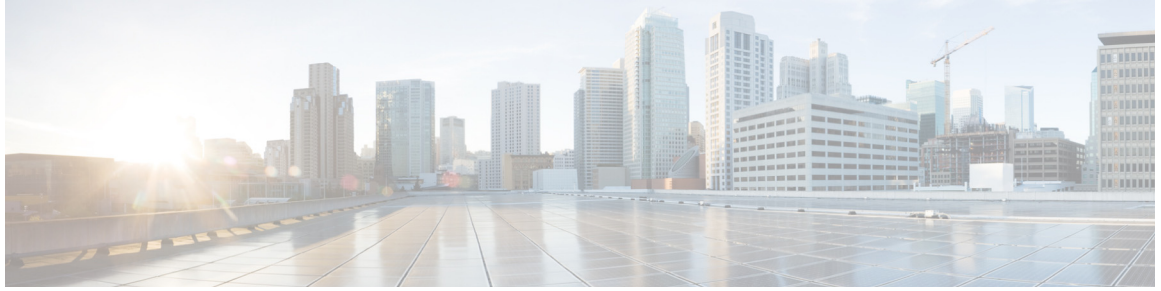
```
switch# configure terminal
switch(config)# monitor session 5 type erspan-source
switch(config-erspan-src)# vrf default
switch(config-erspan-src)#
```

This example shows how to configure a VRF instance for the ERSPAN destination:

```
switch# configure terminal
switch(config)# monitor session 2 type erspan-destination
switch(config-erspan-dst)# vrf default
switch(config-erspan-dst)#
```

Related Commands	Command	Description
	<b>ip ttl</b>	Applies an access control group to an ERSPAN source session.
	<b>monitor-session</b>	Enters the monitor configuration mode for configuring an ERSPAN or SPAN session for analyzing traffic between ports.





# X Commands

---

This chapter describes the Cisco NX-OS system management commands that begin with the letter X.

# xml server max-session

To configure the number of allowed XML server sessions, use the **xml server max-session** command. To reset the number to the default, use the **no** form of this command.

**xml server max-session** *max-sessions*

**no xml server max-session** *max-sessions*

<b>Syntax Description</b>	<i>max-sessions</i> Maximum number of allowed XML server sessions. The range is from 1 to 8. The default is 8.				
<b>Defaults</b>	The XML server sessions allowed is 8.				
<b>Command Modes</b>	Global configuration mode (config)				
<b>Supported User Roles</b>	network-admin vdc-admin				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
<b>Usage Guidelines</b>	This command does not require a license.				
<b>Examples</b>	<p>This example shows how to configure the number of allowed XML server sessions:</p> <pre>switch(config)# <b>xml server max-session 4</b></pre> <p>This example shows how to reset the number of allowed XML server sessions to the default:</p> <pre>switch(config)# <b>no xml server max-session 4</b></pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show xml server status</b></td> <td>Displays information about the status of the XML server.</td> </tr> </tbody> </table>	Command	Description	<b>show xml server status</b>	Displays information about the status of the XML server.
Command	Description				
<b>show xml server status</b>	Displays information about the status of the XML server.				



# xml server terminate session

To terminate an XML server session, use the **xml server terminate session** command.

**xml server terminate session** *session\_id*

<b>Syntax Description</b>	<i>session_id</i> Session number. The range is from 0 to 2147483647.				
<b>Defaults</b>	None				
<b>Command Modes</b>	Any command mode				
<b>SupportedUserRoles</b>	network-admin network-operator vdc-admin vdc-operator				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(1)	This command was introduced.
Release	Modification				
4.0(1)	This command was introduced.				
<b>Usage Guidelines</b>	This command does not require a license.				
<b>Examples</b>	<p>This example shows how to terminate an XML server session:</p> <pre>switch(config)# <b>xml server terminate session 3</b></pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show xml server status</b></td> <td>Displays information about the status of the XML server.</td> </tr> </tbody> </table>	Command	Description	<b>show xml server status</b>	Displays information about the status of the XML server.
Command	Description				
<b>show xml server status</b>	Displays information about the status of the XML server.				

# xml server timeout

To configure the XML server session timeout, use the **xml server timeout** command. To reset the timeout to the default, use the **no** form of this command.

```
xml server timeout timeout [session_id]
```

```
no xml server timeout timeout [session_id]
```

Syntax Description	
<i>timeout</i>	Timeout in seconds. The range is from 0 to 1200. The default is 1200.
<i>session_id</i>	(Optional) XML server session number. The range is from 0 to 2147483647.

**Defaults** The timeout is 1200 seconds.

**Command Modes** Global configuration mode (config)

**Supported User Roles** network-admin  
vdc-admin

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

**Usage Guidelines** You can apply the XML server timeout only to active sessions.  
This command does not require a license.

**Examples** This example shows how to configure the XML server timeout for active sessions:

```
switch(config)# xml server timeout 800
```

This example shows how to reset the timeout to the default:

```
switch(config)# no xml server timeout 800
```

# xml server validate

To validate XML documents, use the **xml server validate** command. To disable XML document validation, use the **no** form of this command.

```
xml server validate {all | session_id}
```

```
no xml server validate {all | session_id}
```

Syntax Description	all	Validates all sessions.
	<i>session_id</i>	Session number. The range is from 0 to 2147483647.

**Defaults** Disabled

**Command Modes** Any command mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

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

**Usage Guidelines** You can validate XML documents only for active sessions.  
This command does not require a license.

**Examples** This example shows how to validate XML documents for all active sessions:

```
switch(config)# xml server validate all
```

This example shows how to disable validation of XML documents for all sessions:

```
switch(config)# no xml server validate all
```

# xmlin

To install the XMLIN tool on the device and generate equivalent Network Configuration (NETCONF) formats of all CLI commands entered in this mode, use the **xmlin** command.

## xmlin

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

**Defaults** None

**Command Modes** EXEC mode

**SupportedUserRoles** network-admin  
network-operator  
vdc-admin  
vdc-operator

Command History	Release	Modification
	6.2(2)	This command was introduced.

**Usage Guidelines** The XMLIN tool converts CLI commands to the NETCONF protocol format. NETCONF is a network management protocol that provides mechanisms to install, manipulate, and delete the configuration of network devices. It uses XML-based encoding for configuration data and protocol messages. The Cisco NX-OS implementation of the NETCONF protocol supports the following protocol operations: <get>, <edit-config>, <close-session>, <kill-session>, and <exec-command>.

The XMLIN tool converts **show**, EXEC, and configuration commands to corresponding NETCONF <get>, <exec-command>, and <edit-config> requests. You can enter multiple configuration commands into a single NETCONF <edit-config> instance.

Note the following restrictions:

- In NETCONF, <edit-config> requests cannot consist of any **show** commands.
- In each <get-config> instance, only one **show** command is allowed.



### Note

Although the XMLIN tool is usually capable of generating NETCONF instances of commands even if the corresponding feature sets or the required hardware capabilities are not available on the device, you might have to install some feature sets before entering the **xmlin** command.

The XMLIN tool also converts the output of **show** commands to XML format by using the *show-command* | **xmlin** command.

Ensure the XMLIN tool is installed before you use the *show-command* | **xmlin** command.

**Note**

XMLIN requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

**Examples**

This example shows how the XMLIN tool is installed on the device and used to convert a set of configuration commands to an <edit-config> instance:

```
switch# xmlin
*****
Loading the xmlin tool. Please be patient.
*****
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright © 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch(xmlin)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)(xmlin)# interface ethernet 2/1
% Success
switch(config-if-verify)(xmlin)# cdp enable
% Success
switch(config-if-verify)(xmlin)# end
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:configure_"
xmlns:m="http://www.cisco.com/nxos:6.2.2.:_exec"
xmlns:ml="http://www.cisco.com/nxos:6.2.2.:configure__if-eth-base" message-id="1">
<nf:edit-config>
  <nf:target>
    <nf:running/>
  </nf:target>
<nf:config><nf:running/>
</nf:target>
<nf:config>
  <m:configure>
    <m:terminal>
      <interface>
        <__XML__PARAM__interface>
          <__XML__value>Ethernet2/1</__XML__value>
          <m1:cdp>
            <m1:enable/>
          </m1:cdp>
        </__XML__PARAM__interface>
      </interface>
    </m:terminal>
  </m:configure>
</nf:config>
</nf:edit-config>
</nf:rpc>
]]>]]>
```

This example shows how to convert the output of the **show interface brief** command to XML:

```
switch# show interface brief | xm1in
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:if_manager"

message-id="1">
  <nf:get>
    <nf:filter type="subtree">
      <show>
        <interface>
          <brief/>
        </interface>
      </show>
    </nf:filter>
  </nf:get>
</nf:rpc>
]]>]]>
```