

S Commands

- salt (sa configuration submode), on page 5
- san-ext-tuner enable, on page 6
- santap module, on page 8
- scaling batch enable, on page 10
- scheduler, on page 11
- scsi-flow distribute, on page 14
- scsi-flow flow-id, on page 15
- scsi-target, on page 17
- sdv abort vsan, on page 19
- sdv commit vsan, on page 20
- sdv enable, on page 21
- sdv virtual-device name, on page 22
- secure-erase abort job, on page 23
- secure-erase create algorithm, on page 24
- secure-erase create job, on page 25
- secure-erase create-vi vsan, on page 26
- secure-erase destroy algorithm, on page 27
- secure-erase destroy job, on page 28
- secure-erase destroy-vi vsan, on page 29
- secure-erase start job, on page 30
- secure-erase stop job, on page 31
- secure-erase validate job, on page 32
- security-mode, on page 33
- send, on page 34
- sensor-group, on page 35
- server, on page 36
- server (trustpoint-est submode), on page 37
- server (configure session submode), on page 39
- server (DMM job configuration submode), on page 40
- server (iSNS profile configuration mode), on page 41
- server (radius configuration), on page 42
- server (tacacs+ configuration), on page 43
- set (IPsec crypto map configuration submode), on page 44

- set interface preference-strict (fcroute-map configuration submode), on page 46
- setup, on page 47
- setup ficon, on page 48
- setup sme, on page 49
- shared-keymode, on page 50
- shutdown, on page 51
- shutdown (Cisco SME and IOA cluster configuration submode), on page 52
- shutdown (interface configuration submode), on page 53
- site-id, on page 54
- sleep, on page 55
- sme, on page 56
- snmp port, on page 57
- snmp-server, on page 58
- snmp-server aaa-user cache-timeout, on page 60
- snmp-server aaa exclusive-behavior enable, on page 61
- snmp-server community, on page 62
- snmp-server contact, on page 63
- snmp-server enable traps, on page 64
- snmp-server enable traps fcdomain, on page 67
- snmp-server enable traps link cisco, on page 68
- snmp-server enable traps zone, on page 69
- snmp-server globalEnforcePriv, on page 70
- snmp-server host, on page 71
- snmp-server location, on page 73
- snmp-server tcp-session, on page 74
- snmp-server traps entity fru, on page 75
- snmp-server user, on page 76
- snsr-grp, on page 78
- source, on page 80
- span max-queued-packets, on page 82
- span session, on page 83
- span session source interface, on page 85
- special-frame, on page 86
- ssh, on page 87
- ssh {ciphers | macs | keytypes | kexalgos| cipher-mode | login-attempts |login-gracetime |rekey } all, on page 89
- ssh connect, on page 92
- ssh idle-timeout, on page 93
- ssh key, on page 94
- ssh name, on page 96
- ssh server enable, on page 98
- ssl, on page 99
- ssm enable feature, on page 100
- ssm upgrade delay, on page 103
- static (iSCSI initiator configuration and iSLB initiator configuration), on page 104
- stop, on page 106

- storage (DMM job configuration submode), on page 107
- streetaddress, on page 108
- subscription, on page 109
- suspend, on page 110
- switchname, on page 112
- switchport auto-negotiate, on page 113
- switchport beacon, on page 114
- switchport description, on page 115
- switchport duplex, on page 116
- switchport encap, on page 117
- switchport fcbbscn, on page 118
- switchport fcrxbbcredit, on page 120
- switchport fcrxbufsize, on page 122
- switchport fec, on page 123
- switchport fec tts, on page 125
- switchport fill-pattern, on page 127
- switchport ignore, on page 128
- switchport ingress-rate, on page 130
- switchport initiator id, on page 131
- switchport link-diag, on page 132
- switchport max-npiv-limit, on page 134
- switchport mode, on page 135
- switchport mtu, on page 137
- switchport link-negotiation early-tc, on page 138
- switchport owner, on page 139
- switchport promiscuous-mode, on page 140
- switchport proxy-initiator, on page 141
- switch-priority, on page 143
- switchport rate-mode, on page 144
- switchport speed, on page 148
- switchport trunk allowed vsan, on page 150
- switchport trunk-max-npiv-limit, on page 151
- switchport trunk mode, on page 152
- switch-wwn, on page 154
- system cores, on page 156
- system counter , on page 157
- system default interface congestion mode, on page 159
- system default interface congestion timeout, on page 160
- system default interface pause mode, on page 162
- system default interface pause timeout, on page 163
- system default rib ipfc-mcast-deny, on page 164
- system default switchport, on page 165
- system-default-tx-credits-double-queue, on page 167
- system default zone default-zone permit, on page 168
- system default zone distribute full, on page 169
- system default zone gs, on page 170

- system default zone mode enhanced, on page 171
- system default zone smart-zone, on page 172
- system delayed-traps enable mode, on page 173
- system delayed-traps timer, on page 174
- system hap-reset, on page 175
- system health (configuration mode), on page 176
- system health cf-crc-check, on page 179
- system health cf-re-flash, on page 180
- system health clear-errors, on page 181
- system health external-loopback, on page 183
- system health internal-loopback, on page 185
- system health module, on page 187
- system health serdes-loopback, on page 190
- system heartbeat, on page 192
- system kernel core, on page 193
- system memlog, on page 194
- system port pacer mode F interface-login-threshold, on page 195
- system startup-config, on page 196
- system statistics reset, on page 197
- system switchover (configuration mode), on page 198
- system switchover (EXEC mode), on page 199
- system timeout congestion-drop, on page 200
- system timeout no-credit-drop, on page 202
- system timeout slowport-monitor, on page 204
- system timestamp format, on page 205
- system trace, on page 208
- system transceiver power-control, on page 209
- system watchdog, on page 210

salt (sa configuration submode)

To configure the salt for the Security Association (SA), use the key command. To delete the salt from the SA, use the no form of the command.

salt *salt*
no salt *salt*

Syntax Description

salt	Specifies the salt for encryption. The range is from 0x0 to 0xffffffff.

Command Default

None.

Command Modes

Configuration submode

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the salt for the current SA:

```
switch# config t
switch(config)# fcsp esp sa 257
This is a Early Field Trial (EFT) feature.  Please do not use this in a producti
on environment. Continue Y/N ? [no] y
switch(config-sa)# salt 0x0
```

Related Commands

Command	Description
fcsp enable	Enables FC-SP.
show fcsp interface	Displays FC-SP related information for a specific interface.

san-ext-tuner enable

To enable the IP Network Simulator to simulate a variety of data network conditions, use the **san-ext-tuner enable** command.

san-ext-tuner enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The IP Network Simulator tool is used for network simulation and is supported on the 8-port IP Storage Services (IPS-8) module and 4-port IP Storage Services (IPS-4) module only. You must also have either the SAN extension over IP package for IPS-8 modules (SAN_EXTN_OVER_IP) or SAN extension over IP package for IPS-4 modules (SAN_EXTN_OVER_IP_IPS4), so that you can enable the SAN Extension Tuner, a prerequisite for enabling and using the network simulator.

You must have a pair of Gigabit Ethernet ports dedicated for each Ethernet path requiring simulation; these ports cannot provide FCIP or iSCSI functionality while simulation occurs. The remaining ports that are not performing network simulations can run FCIP or iSCSI. Ports dedicated to network simulation must be adjacent, and always begin with an odd-numbered port. For example, GE 1/1 and GE 1/2 would be a valid pair, while GE 2/2 and GE 2/3 would not.



Note This command is not supported on the Cisco MDS 9124 switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.

Examples

The following example shows how to enable the SAN Extension Tuner and enable a pair of ports for network simulation:

```
switch#
config t
switch(config)#
switch(config)#
san-ext-tuner enable
switch(config)#
exit
switch#
switch#
ips netsim enable interface gigabitethernet 2/3 gigabitethernet 2/4
```

Related Commands

Command	Description
show ips netsim	Displays a summary of the interfaces that are currently operating in network simulation mode.
show ips statsnetsim ingress	Displays the parameters and statistics of interfaces currently operating in network simulation mode for the specified direction of traffic.

santap module

To configure the mapping between the Storage Services Module (SSM) and the VSAN where the appliance is configured, use the **santap module** command in configuration mode. To disable this feature, use the **no** form of the command.

santap module *slot-number* {**appl-vsan** *vsan-id* [**cvt-name** *cvt-name*] | **dvt target-pwwn** *target-pwwn* **target-vsan** *target-vsan-id* **dvt-name** *dvt-name* **dvt-vsan** *dvt-vsan-id* [**dvt-port** *port-number*] [**lun-size-handling enable**/**disable**] [**io-timeout** *timeout-value*]}
no santap module *slot-number* {**appl-vsan** *vsan-id* [**cvt-name** *cvt-name*] | **dvt target-pwwn** *target-pwwn*}

Syntax Description

slot-number	Specifies the slot number of the SSM where the control virtual target (CVT) is created.
appl-vsan vsan-id	Specifies the appliance VSAN identification number used to communicate with the appliance. The range is 1 to 4093.
cvt-name *cvt-name*	(Optional) Specifies the control virtual target (CVT) name. The maximum size is 80 characters.
dvt	Configures the data virtual target (DVT).
target-pwwn *target-pwwn*	Specifies the target pWWN for the DVT. The format is *hh:hh:hh:hh:hh:hh:hh:hh.*
target-vsan *target-vsan-id*	Specifies the target VSAN for the DVT. The range for the real *target-vsan-id is 1 through 4093.*
dvt-name *dvt-name*	Specifies the DVT name. The maximum size is 80 characters.
dvt-vsan *dvt-* vsan-id	Specifies the DVT VSAN. The range for the *dvt-vsan-id is 1 through 4093.*
dvt-port port-number	(Optional) Specifies the DVT port. The range for the port number is 1 through 32.
lun-size-handling enable/disable	(Optional) Enables or disables LUN size handling. Specify 1 to enable or 0 to disable LUN size handling, with the default being enable.
io-timeout *timeout-value*	(Optional) Specifies the I/O timeout value. The range is 10 to 200 seconds, with the default being 10 seconds.

Command Default

Disabled.

The IO-timeout is 10 seconds.

Lun-size-handling is Enabled.

Command Modes

onfiguration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.
3.0(1)	Added the following options: **cvt-name**, **dvt**, **target-pwwn**, **target-vsan**, **dvt-name**, **dvt-vsan**, **dvt-port**, **lun-size-handling**, and **io-timeout**.

Usage Guidelines

To access this command, you must first enable the SANTap feature on the SSM using the ssm enable feature command.

When the **lun-size-handling** option is set (enabled), the maximum logical block addressing (LBA) for DVT LUN is set to 2 TB. As a result, there is no issue with LUN resizing.

Note You can delete **dvt target-pwwn using the no santap module** *slot* **dvt target-pwwn command. Other dvt options are not supported by the no form of the command.**

Examples

The following example shows the configuration of the SSM where the SANTap feature is enabled and the VSAN used to communicate with the appliance:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# santap module 1 appl-vsan 1
```

Related Commands

Command	Description
show santap module	Displays the configuration and statistics of the SANTap feature.
ssm enable feature	Enables the SANTap feature on the SSM.

scaling batch enable

To enable scalability in the Cisco SME configuration, use the **scaling batch enable** command. To disable this feature, use the no form of the command.

scaling batch enable
no scaling batch enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Cisco SME cluster onfiguration submode

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable Cisco SME scalability:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# scaling batch enable
switch(config-sme-cl)#
```

Related Commands

Command	Description
show santap module	Displays the configuration and statistics of the SANTap feature.
ssm enable feature	Enables the SANTap feature on the SSM.

scheduler

To schedule a maintenance job, use the **scheduler** command. To disable a job, use the no form of the 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

aaa-authentication	Specifies AAA credentials for AAA authentication of a remote user.
username	(Optional) Specifies the remote user and specifies the username. If the username keyword is not specified in the command, the currently logged-in user's name will be used.
username	(Optional) Specifies the remote user username.
password	Specifies the password of the logged-in remote user for AAA authentication.
0	(Optional) Specifies that the password is in clear text.
7	(Optional) Specifies that the password is encrypted.
password	Specifies the remote user's password. If the encryption level was not specified (0 or 7), the supplied password will be encrypted.
job name	Specifies a scheduler job.
job-name	Specifies the name of the scheduler job. The maximum length is 31 characters.
logfile size	Specifies a log file configuration.
filesize	Specifies the size of the log file. The range is 16 to 1024 KB.
schedule name	Specifies a scheduler schedule.
schedule-name	Specifies the name of the schedule. The maximum length is 31 characters.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
NX-OS 4.1(3)	Deleted a note from the Usage Guidelines.
NX-OS 4.1(1b)	Added a note to the Usage Guidelines.
2.0(x)	This command was introduced.

Usage Guidelines

Scheduler job configurations may not be edited. They need to be deleted and reconfigured to make changes. Jobs may comprise of multiple commands which can be entered in a single line by using ";" as the delimiter between commands.

A user's credentials are checked by the scheduler before allowing them to create, delete or run a scheduled jobs. Use the scheduler aaa-authetication command to configure a remote user's (a user without local credentials) credentials. The scheduler uses these credentials to verify that the user account is still active on the AAA server each time before it starts the job.

To use the command scheduler. You do not need to obtain any license.

Examples

The following example shows how to enable the scheduler command:

```
switch# config t
```

switch(config)# feature scheduler

switch(config)#

The following example shows how to specify the password for the currently logged-in remote user:

```
switch# config t
switch(config)# scheduler aaa-authentication password newpwd
switch(config)#
```

The following example shows how to specify a clear text password for the currently logged-in remote user:

```
switch# config t
switch(config)# scheduler aaa-authentication password 0 X12y34Z56a
switch(config)#
```

The following example shows how to specify a name and password for a remote user:

```
switch# config t
switch(config)# scheduler aaa-authentication username newuser password newpwd3
switch(config)#
```

The following example shows how to specify scheduler logfile size:

switch(config)# scheduler logfile size 512 switch(config)#

The following example shows how to define a name for the schedule and enters the submode for that schedule:

```
switch(config)# scheduler schedule name my_timetable
switch(config-schedule)#
```

The following example shows how to specify a schedule to run jobs:

```
switch(config-schedule)# time daily 1:23
switch(config-schedule)#
```

The following example shows how to define a job that uses variables:

```
switch(config)# scheduler job name my_job
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/
switch(config-job)# exit
switch(config)#
```

Related Commands

Command	Description
cli var	Defines a variable.
feature scheduler	Enables the scheduler.
job name	Specifies a scheduler job.
show scheduler time	Displays scheduler information.
time	Specifies a schedule start time.

scsi-flow distribute

To enable SCSI flow distribution through CFS, use the scsi-flow distribute command. To disable the SCSI flow distribution, use the **no** form of the command.

scsi-flow distribute
no scsi-flow distribute

Syntax Description

This command has no arguments or keywords.

Command Default

SCSI flow distribution is enabled.

Command Modes

Configuration mode

Command History

Release	Modification
2.0(2)	This command was introduced.

Usage Guidelines

You must enable the SCSI flow feature on the Storage Services Module (SSM) before you can configure an SCSI flow. Use the **ssm enable feature module** *slot-number* command to enable the SCSI flow feature on the SSM.

Examples

The following example enables distribution of SCSI flow services using CFS:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# scsi-flow distribute
```

The following example disables distribution of SCSI flow services:

```
switch(config)# no scsi-flow distribute
```

Related Commands

Command	Description
show santap module	Displays SCSI flow configuration and status.
ssm enable feature	Enables the SCSI flow feature on the SSM.

scsi-flow flow-id

To configure SCSI flow services, use the scsi-flow flow-id command. To disable the SCSI flow services, use the **no** form of the command.

scsi-flow flow-id *flow-id* {**initiator-vsan** *vsan-id* **initiator-pwwn wwn target-vsan** *vsan-id* **target-pwwn wwn** | **statistics** | **write-acceleration** [**buffers count**]}
no scsi-flow flow-id flow-id {**statistics** | **write-acceleration**}

Syntax Description

flow-id	Configures the SCSI flow identification number. The range is 1 to 65535.
initiator-vsan *vsan-id*	Specifies the initiator VSAN identification number. The range is 1 to 4093.
initiator-pwwn *wwn*	Configures initiator side pWWN.
target-vsan *vsan-id*	Configures target VSAN identification number of the SCSI flow.
target-pwwn *wwn*	Configures the target side pWWN.
statistics	Enables statistics gathering.
write-acceleration	Enables write acceleration.
buffers *count*	(Optional) Configures the write acceleration buffer count. The range is 1 to 40000 and the default is 1024.

Command Default

SCSI flow services are disabled.

Command Modes

Configuration mode

Command History

Release	Modification
2.0(2)	This command was introduced.

Usage Guidelines

You must enable the SCSI flow feature on the Storage Services Module (SSM) before you can configure a SCSI flow. Use the **ssm enable feature module** *slot-number* command to enable the SCSI flow feature on the SSM.

Examples

The following example configures an SCSI flow with a flow identifier of 4 and the following attributes:

- Initiator VSAN number—101
- Initiator port WWN—21:00:00:e0:8b:05:76:28
- Target VSAN number—101
- Target port—WWN 21:00:00:20:37:38:67:cf

```
switch# config terminal
switch(config)# scsi-flow flow-id 4 initiator-vsan 101 initiator-pwwn 21:00:00:e0:8b:05:76:28
 target-vsan 101 target-pwwn 21:00:00:20:37:38:67:cf
```

The following example disables a SCSI flow with a flow identifier of 4:

```
switch(config)# no scsi-flow flow-id 4
```

The following example configures SCSI flow 4 to gather statistics about the SCSI flow:

```
switch(conf)# scsi-flow flow-id 4 statistics
```

The following example disables the statistics gathering feature on SCSI flow 4:

```
switch(conf)# no scsi-flow flow-id 4 statistics
```

The following example configures SCSI flow 4 with write acceleration:

```
switch(conf)# scsi-flow flow-id 4 write-acceleration
```

The following example configures SCSI flow 4 with write acceleration and buffers of 1024 credits:

```
switch(conf)# scsi-flow flow-id 4 write-acceleration buffer 1024
```

The following example disables the write acceleration feature on SCSI flow 4:

```
switch(conf)# no
 scsi-flow flow-id 4 write-acceleration
```

Related Commands

Command	Description
show scsi-flow	Displays SCSI flow configuration and status.
ssm enable feature	Enables the SCSI flow feature on the SSM.

scsi-target

To configure SCSI target discovery, use the **scsi-target** command in configuration mode. To remove SCSI target discovery, use the **no** form of the command.

scsi-target {**auto-poll** [**vsan** *vsan-id*] | **discovery** | **ns-poll** [**vsan** *vsan-id*] | **on-demand** [**vsan** *vsan-id*]}
no scsi-target {**auto-poll** [**vsan** *vsan-id*] | **discovery** | **ns-poll** [**vsan** *vsan-id*] | **on-demand** [**vsan** *vsan-id*]}

Syntax Description

auto-poll	Configures SCSI target auto polling globally or per VSAN.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is 1 to 4093.
discovery	Configures SCSI target discovery.
ns-poll	Configures SCSI target name server polling globally or per VSAN.
on-demand	Configures SCSI targets on demand globally or per VSAN.

Command Default

SCSI target discovery for each option is on.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1a)	This command was introduced.

Usage Guidelines

Automatic global SCSI target discovery is on by default. Discovery can also be triggered for specific VSANs using on-demand, name server polling, or auto-polling options. All options are on by default. Use the **no scsi-target discovery** command to turn off all discovery options. You can also turn off specific options by using the **no** form of the command.

Examples

The following example configures SCSI target auto-polling discovery for VSAN 1:

```
switch# config t
switch(config)# scsi-target auto-poll vsan 1
```

The following example removes SCSI target auto-polling discovery for VSAN 1:

```
switch# config t
switch(config)# no scsi-target auto-poll vsan 1
```

The following example configures an SCSI target discovery:

```
switch# config t
switch(config)# scsi-target discovery
```

The following example removes a SCSI target discovery:

```
switch# config t
switch(config)# no scsi-target discovery
```

The following example configures SCSI target ns-polling discovery for VSAN 1:

```
switch# config t
switch(config)# scsi-target ns-poll vsan 1
```

The following example removes SCSI target ns-polling discovery for VSAN 1:

```
switch# config t
switch(config)# no scsi-target ns-poll vsan 1
```

The following example configures SCSI target on-demand discovery for VSAN 1:

```
switch# config t
switch(config)# scsi-target on-demand vsan 1
```

The following example removes SCSI target on-demand discovery for VSAN 1:

```
switch# config t
switch(config)# no scsi-target on-demand vsan 1
```

Related Commands

Command	Description
discover scsi-target	Discovers SCSI targets on local storage to the switch or remote storage across the fabric.
show scsi-target	Displays information about existing SCSI target configurations.

sdv abort vsan

To terminate an SDV configuration for a specified VSAN, use the **sdv abort vsan** command in configuration mode.

sdv abort vsan *vsan-id*

Syntax Description

vsan-id	Specifies the number of the VSAN. The range is 1 to 4093.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
4.x	This command was deprecated.
3.1(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable SDV using the **sdv enable** command.

Examples

The following example shows how to terminate an SDV configuration for a specified VSAN:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# sdv abort vsan 2
```

Related Commands

Command	Description
sdv enable	Enables SDV.
show sdv database	Displays the SDV database.

sdv commit vsan

To commit an SDV configuration to a specified VSAN, use the **sdv commit vsan** command in configuration mode. To remove the SDV configuration for a specified VSAN, use the **no** form of the command.

sdv commit vsan *vsan-id*
no sdv commit vsan *vsan-id*

Syntax Description

vsan-id	Specifies the number of the VSAN. The range is 1 to 4093.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
4.x	This command was deprecated.
3.1(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable SDV using the **sdv enable** command.

Examples

The following example shows how to commit an SDV configuration to a specified VSAN:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# sdv commit vsan 2
```

The following example shows how to uncommit an SDV configuration from a specified VSAN:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no sdv commit vsan 2
```

Related Commands

Command	Description
sdv enable	Enables SDV.
show sdv database	Displays the SDV database.

sdv enable

To enable SDV on the switch, use the **sdv enable** command in configuration mode. To disable SDV, use the **no** form of the command.

sdv enable
no sdv enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
4.x	This command was deprecated.
3.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable SDV:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sdv enable
```

The following example shows how to disable SDV:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no sdv enable
```

Related Commands

Command	Description
show sdv database	Displays the SDV database.
show vritual-device	Displays the virtual devices.

sdv virtual-device name

To create a virtual device name for a specified VSAN, use the **sdv virtual-device name** command in configuration mode. To remove the name, use the **no** form of the command.

sdv virtual-device name *device-name* **vsan** *vsan-id*
no sdv virtual-device name *device-name* **vsan** *vsan-id*

Syntax Description

device-name	Specifies the name of the device. The maximum size is 32.
vsan *vsan-id*	Specifies the number of the VSAN. The range is 1 to 4093.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
4.x	This command was deprecated.
3.1(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable SDV using the **sdv enable** command.

No more than 1000 virtual targets can be created in a single VSAN.

No more than 128 devices can be defined as virtual devices.

Examples

The following example shows how to create a virtual device name for a VSAN, and then specify both the primary and secondary pWWNs:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sdv virtual-device name vdev1 vsan 2
switch(config-sdv-virt-dev)# pwwn 21:00:00:04:cf:cf:45:40 primary
switch(config-sdv-virt-dev)# pwwn 21:00:00:04:cf:cf:38:d6
```

The following example shows how to remove the virtual device name:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no sdv virtual-device name vdev1 vsan 2
```

Related Commands

Command	Description
sdv enable	Enables SDV.
show sdv database	Displays the SDV database.

secure-erase abort job

To terminate a Secure Erase job, use the **secure-erase abort job** command in configuration mode.

secure-erase *module-id* **abort job** *job-id*

Syntax Description

module-id	Specifies the desired module number of the SSM on which Secure Erase is provisioned.
job-id	Specifies the job ID of the target.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

This command does not wait for the completion of current patterns. A terminated job cannot be restarted.

A job can be terminated only when it has one or more sessions in the running state.

Examples

The following example shows how to abort a Secure Erase job:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 abort job 1
```

Related Commands

Command	Description
secure-erase start job	Restarts all sessions in a job.
secure-erase stop job	Stops all sessions in a job.
secure-erase validate job	Validates a job in a session.

secure-erase create algorithm

To configure a Secure Erase algorithm on a specific slot of the intelligent linecard where Secure Erase is provisioned, use the **secure-erase module create algorithm** command in configuration mode.

secure-erase module *module-id* **create algorithm** *algorithm-id*

Syntax Description

module-id	Specifies the desired slot number of the intelligent linecard on which Secure Erase is provisioned.
algorithm-id	Specifies the algorithm ID. The range is 0 to 9.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to create a Secure Erase algorithm:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 create algorithm 3
```

Related Commands

Command	Description
secure-erase create-vi vsan	Creates a VI for a specific VSAN.

secure-erase create job

To create a Secure Erase job, use the **secure-erase create job** command in configuration mode.

secure-erase module *module-id* **create job** *job-id*

Syntax Description

module *module-id*	Specifies the desired module number of the Storage Services Module (SSM) on which Secure Erase is provisioned.
job-id	Specifies a unique number to identify a Secure Erase job. The range is 1 to 9999. **Note** You will be prompted to choose a different ID if the job ID chosen already exists.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

A Secure Erase job contains the following information:

- The target enclosure where Secure Erase needs to be performed. Multiple target ports spanning multiple VSANs can be a part of one target enclosure.
- Multiple target ports, VIs, and Secure Erase sessions can be added. These target ports and VIs can be a part of different VSANs.

Examples

The following example shows how to create a Secure Erase job:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 create job 1
```

Related Commands

Command	Description
add-tgt job	Defines a target enclosure and adds multiple target ports for a specific Secure Erase job.

secure-erase create-vi vsan

To create a VI for a specific VSAN, use the **secure-erase create-vi vsan** command in configuration mode.

secure-erase module *module-id* **create-vi vsan** *vsan-id*

Syntax Description

module *module-id*	Specifies the desired slot number of the SSM on which Secure Erase is provisioned.
vsan-id	Specifies the VSAN ID of the target port being added.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

You do not need to provide the job ID because VIs can be used commonly across jobs.

Examples

The following example shows how to create VIs for a VSAN:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 create-vi vsan 1
```

Related Commands

Command	Description
create job	Creates a Secure Erase job.

secure-erase destroy algorithm

To destroy a Secure Erase algorithm, use the **secure-erase destroy algorithm** command in configuration mode.

secure-erase module *module-id* **destroy algorithm** *algorithm-id*

Syntax Description

module *module-id*	Displays the slot number of the SSM on which Secure Erase is provisioned.
algorithm-id	Displays the algorithm ID. The range is 0 to 9.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to destroy an algorithm:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 destroy algorithm 1
```

Related Commands

Command	Description
secure-erase destroy- vi vsan	Destroys a Secure Erase VSAN.

secure-erase destroy job

To destroy a Secure Erase job, use the **secure-erase destroy job** command in configuration mode.

secure-erase *module-id* **destroy job** *job-id*

Syntax Description

module-id	Specifies the desired module number of the SSM on which Secure Erase is provisioned.
job-id	Specifies the job ID of the target.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

This command destroys a Secure Erase job. A job can be destroyed only when there are no active sessions running.

Examples

The following example shows how to validate a Secure Erase job:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 destroy job 1
```

Related Commands

Command	Description
secure-erase start job	Starts all sessions in a job.
secure-erase stop job	Stops all sessions in a job.

secure-erase destroy-vi vsan

To destroy a VI for a specific VSAN, use the **secure-erase destroy-vi vsan** command in configuration mode.

secure-erase module *module-id* **destroy-vi vsan** *vsan-id*

Syntax Description

module *module-id*	Displays the slot number of the SSM on which Secure Erase is provisioned.
vsan-id	Displays the VSAN-ID of the target.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to destroy a VSAN:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 destroy-vi vsan 1
```

Related Commands

Command	Description
secure-erase destroy algorithm	Destroys a Secure Erase algorithm.

secure-erase start job

To restart all sessions in a job, use the **secure-erase start job** command in configuration mode.

secure-erase module *module-id* **start job** *job-id*

Syntax Description

module *module-id*	Specifies the desired module number of the SSM on which Secure Erase is provisioned.
job-id	Starts a specific job ID of the target.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

This command starts all sessions in a job. If the active sessions have reached the maximum limit, the remaining sessions are queued. The queued sessions start when one or more sessions are complete or terminated.

A job can be started only when it has one or more sessions in the stopped state or ready state.

Examples

The following example shows how to start a session in a Secure Erase job:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 start job 1
```

Related Commands

Command	Description
secure-erase stop job	Stops all sessions in a job.

secure-erase stop job

To stop all sessions in a job, use the **secure-erase stop job** command in configuration mode.

secure-erase *module-id* **stop job** *job-id*

Syntax Description

module-id	Specifies the desired module number of the SSM on which Secure Erase is provisioned.
job-id	Stops the specific job ID of the target.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

This command waits for the completion of the current pattern and pauses the pattern sequence. A stopped job can be restarted.

A job can be stopped only when it has one or more sessions in the running state.

Examples

The following example shows how to stop a session in a Secure Erase job:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 stop job 1
```

Related Commands

Command	Description
secure-erase start job	Restarts all sessions in a job.

secure-erase validate job

To validate a Secure Erase job, use the **secure-erase validate job** command in configuration mode.

secure-erase *module-id* **validate job** *job-id*

Syntax Description

module-id	Specifies the desired module number of the SSM on which Secure Erase is provisioned.
job-id	Specifies the job ID of the target.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to validate a Secure Erase job:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 validate job 1
```

Related Commands

Command	Description
secure-erase abort job	Terminates a job in a session.
secure-erase start job	Restarts all sessions in a job.
secure-erase stop job	Stops all sessions in a job.

security-mode

To configure the Cisco SME security settings, use the **security-mode** command. To delete the security settings, use the **no** form of the command.

security-mode {**basic** | **standard** | **advanced schema threshold** *threshold* **total** *total*}
no security-mode {**basic** | **standard** | **advanced schema threshold** *threshold* **total** *total*}

Syntax Description

basic	Sets the Cisco SME security level to basic.
standard	Sets the Cisco SME security level to standard.
advanced	Sets the Cisco SME security level to advanced.
schema	Configures the recovery schema.
threshold *threshold*	Configures the recovery schema threshold. The limit is 2-3.
total *total*	Configures the recovery schema total. The limit is 5-5.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets the security mode to basic:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# security-mode basic
```

The following example sets the security mode to advanced:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# security-mode advanced schema threshold 3 total 5
```

Related Commands

Command	Description
show sme cluster	Displays information about the security settings.

send

To send a message to all active CLI users currently using the switch, use the **send** command in EXEC mode.

send *message-text*

Syntax Description

message-text	Specifies the text of your message.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This message is restricted to 80 alphanumeric characters with spaces.

Examples

The following example sends a warning message to all active users about the switch being shut down:

```
switch# send Shutting down the system in 2 minutes. Please log off.
Broadcast Message from admin@excal-112
        (/dev/pts/3) at 16:50 ...
Shutting down the system in 2 minutes. Please log off.
```

sensor-group

To create a sensor group and enter sensor group configuration mode, use the **sensor-group** command. To remove the sensor group, use the **no** form of this command.

sensor-group *id*

no sensor-group *id*

Syntax Description

id	Sensor group ID. Range is from 1 to 4095.

Command Default

No sensor group exists.

Command Modes

Telemetry configuration mode (config-telemetry)

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

Currently, only numeric sensor group ID values are supported. The sensor group defines nodes that are monitored for telemetry reporting.

Examples

This example shows how to add a sensor group:

```
switch# configure
switch(config)# telemetry
switch(config-telemetry)# sensor-group 100
```

This example shows how to remove a sensor group:

```
switch# configure
switch(config)# telemetry
switch(config-telemetry)# no sensor-group 100
```

Related Commands

Command	Description
feature telemetry	Enables the SAN Telemetry Streaming feature.
path	Adds a sensor path of an interface or a query name to a sensor group.
show running-config telemetry	Displays the existing telemetry configuration.
show telemetry	Displays telemetry configuration.
telemetry	Enters SAN Telemetry Streaming configuration mode.

server

To add a server to the server group, use the **server** command. To disable this feature, use the **no** form of the command.

server *ip address or DNS name*
no server*ip addressor DNS name*

Syntax Description

ipaddress or DNS name	Specifies LDAP server name.

Command Default

None.

Command Modes

Configuration submode

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

This CLI is allowed to be configured multiple times for different servers. These servers will be tried sequentially in case of failure with one server. Also the same server can belong to multiple groups.

Examples

The following example shows how to configure LDAP server name:

```
switch(config)# aaa group server ldap a
switch(config-ldap)# server local
Error: specified LDAP server not found, first configure it using ldap-server hos
t... and then retry
switch(config-ldap)#
```

Related Commands

Command	Description
show ldap-server groups	Displays the configured LDAP server groups.

server (trustpoint-est submode)

Use the **server** command to configure the location of the EST server, port number and if it is reached via a proxy. The proxy server is an intermediary that forwards HTTP requests from the MDS switch to the EST server. Use the **no** form of the command to remove the server information.

server *est_server* **port** *port_number* [[**path-segment** *path_segment*] **proxy system**]

no server *est_server* **port** *port_number* [[**path-segment** *path_segment*] **proxy system**]

Syntax Description

est_server	Specifies the server name
port *port_number*	Specifies the port number of the server.
path-segment *path_segment*	Specifies the URL path on the EST server where EST endpoints are hosted.
proxy system	Specifies the connection to the server should be routed through a system-defined proxy rather than connecting directly

Command Default

None.

Command Modes

trustpoint-est configuration submode.

Command History

Release	Modification
9.4(5)	This command was introduced.

Usage Guidelines

If the MDS switch needs to reach the EST server via an HTTP proxy, you must configure the proxy server's FQDN or IP address and its port number. If using domain name ensure that DNS resolution is configured properly.

Examples

```
switch# configure terminal
switch(config)# ip name-server 198.0.100.1
switch(config)# ip domain-lookup
switch(config)# ip domain-name example.com
switch(config)# system proxy http proxy1 port 8443
switch(config)# crypto ca trustpoint engineering-est-tp
switch(config-trustpoint)# management-method est
switch(config-trustpoint-est)# enrollment
switch(config-trustpoint-est)# renew lifetime 90
switch(config-trustpoint-est)# server 192.0.2.123 port 8443 path-segment /certs-eng proxy
system
```

Related Commands

Command	Description
renew lifetime	Configures when to start certificate renewal.

Command	Description
management-method est	Enters EST configuration submode
client-trustpoint	Specifies the trustpoint containing the switch client certificates.
enrollment	Enable automatic switch identity certificate renewal.

server (configure session submode)

To configure a data migration session, use the **server** command in session configuration submode. To remove the data migration session, use then **no** form of the command.

server *pwwn* **src_tgt** *pwwn* **src_lun** *src-lun* **dst_tgt** *pwwn* **dst_lun** *dst-lun*
no server *pwwn* **src_tgt** *pwwn* **src_lun** *src-lun* **dst_tgt** *pwwn* **dst_lun** *dst-lun*

Syntax Description

pwwn	Specifies the pWWN of the server. The format is *hh:hh:hh:hh:hh:hh:hh:hh,* where *h* is a hexadecimal number.
src_tgt *pwwn*	Specifies the pWWN of the source target. The format is *hh:hh:hh:hh:hh:hh:hh:hh* , where *h* is a hexadecimal number.
src_lun *src-lun*	Specifies the source LUN number in hex notation. The range is 0x0 to 0xfff.
dst_tgt *pwwn*	Specifies the pWWNof the destination target. The format is *hh:hh:hh:hh:hh:hh:hh:hh* , where *h* is a hexadecimal number.
dst_lun *dst-lun*	Specifies the destination LUN in hex notation. The range is 0x0 to 0xfff.

Command Default

None.

Command Modes

Configure session submode

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure a source target, source LUN, destination target, and destination LUN in a session:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# dmm module 3 job 1 session
switch(config-session)# server 12:13:1d:1c:2d:2d:3f:3a src_tgt 12:13:1d:1c:2d:2d:3f:3a
src_lun 0x1 dst_tgt 12:13:1d:1c:2d:2d:3f:3a dst_lun 0x5
```

Related Commands

Command	Description
show dmm ip-peer	Displays job information.
show dmm srvr-vt-login	Displays server VT login information.

server (DMM job configuration submode)

To add a server HBA port to the DMM job, use the **server** command in DMM job configuration submode. To remove the server HBA port, use the **no** form of the command.

server vsan *vsan-id* **pwwn** *port-wwn*
no server vsan *vsan-id* **pwwn** *port-wwn*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
pwwn *port-wwn*	Specifies the port worldwide name of the server HBA port. The format is *hh:hh:hh:hh:hh:hh:hh:hh* , where *h* is a hexadecimal number.

Command Default

None.

Command Modes

DMM job configuration submode

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add server information to a DMM job:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# dmm module 3 job 1 create
Started New DMM Job Configuration.
Do not exit sub-mode until configuration is complete and committed
switch(config-dmm-job)# server vsan 3 pwwn 1d:22:3a:21:3c:44:3b:51
switch(config-dmm-job)#
```

Related Commands

Command	Description
show dmm ip-peer	Displays job information.
show dmm srvr-vt-login	Displays server VT login information.

server (iSNS profile configuration mode)

To add a server in an Internet Storage Name Service (iSNS) profile, use the **server** command **in iSNS profile configuration submode.** To delete a server from an iSNS profile, use the **no** form of the command.

server *server-id*
no server *server-id*

Syntax Description

server-id	Specifies the server address. The format is *A.B.C.D*.

Command Default

None.

Command Modes

iSNS profile configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

An iSNS profile can have only one server address. To change the server address, you must delete the current server and add the new one.

Examples

The following example shows how to add a server address to an iSNS profile:

```
switch# config terminal
switch(config)# isns profile name UserProfile
switch(config-isns-profile)# server 10.1.1.1
```

The following example shows how to delete a server address from an iSNS profile:

```
switch# config terminal
switch(config)# isns profile name AdminProfile
switch(config-isns-profile)# no server 10.2.2.2
```

Related Commands

Command	Description
isns-server enable	Enables the iSNS server.
isns profile name	Creates iSNS profiles.
show isns	Displays iSNS information.

server (radius configuration)

To configure a RADIUS server, use the **server** command in RADIUS configuration submode. To discard the configuration, use the **no** form of the command.

server [*ipv4-addressipv6-addressdns name*]
no server [*ipv4-addressipv6-addressdns name*]

Syntax Description

ipv4-address	(Optional) Specifies the RADIUS server IP address in the format *A.B.C.D* .
ipv6-address	(Optional) Specifies the RADIUS server IP address in the format *X:X::X* .
name	(Optional) Specifies the RADIUS DNS server name. The maximum size is 255.

Command Default

None.

Command Modes

RADIUS configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Added the ipv6-address argument.

Usage Guidelines

None.

Examples

The following example shows the **server** command in RADIUS configuration submode:

```
switch# config terminal
switch(config)# aaa group server radius testgroup
switch(config-radius)# server myserver
```

Related Commands

Command	Description
radius-server host	Configures RADIUS server parameters.
show radius-server	Displays RADIUS server configuration parameters.

server (tacacs+ configuration)

To configure a TACACS+ server, use the **server** command in TACACS+ configuration submode. To discard the configuration, use the **no** form of the command.

server [*ipv4-addressipv6-addressdns-name*]
no server [*ipv4-addressipv6-addressdns-name*]

Syntax Description

ipv4-address	(Optional) Specifies the TACACS+ server IP address in the format *A.B.C.D* .
ipv6-address	(Optional) Specifies the TACACS+ server IP address in the format *X:X::X* .
dns-name	(Optional) Specifies the TACACS+ DNS server name. The maximum size is 255.

Command Default

None.

Command Modes

TACACS+ configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Added the ipv6-address argument.

Usage Guidelines

None.

Examples

The following example shows the **server** command in RADIUS configuration submode:

```
switch# config terminal
switch(config)# aaa group server tacacs+ testgroup
switch(config-
tacacs+
)# server myserver
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server configuration parameters.
tacacs-server host	Configures TACACS+ server parameters.

set (IPsec crypto map configuration submode)

To configure attributes for IPsec crypto map entries, use the **set** command **in IPsec crytpo map configuration submode.** To revert to the default values, use the **no** form of the command.

set {**peer** {*ip-address* | **auto-peer**} | **pfs** [**group1** | **group14** | **group2** | **group5**] | **security-association lifetime** {**gigabytes** *number* | **kilobytes** *number* | **megabytes** *number* | **seconds** *number*} | **transform-set** {*set-nameset-name-list*}}
no set {**peer** {*ip-address* | **auto-peer**} | **pfs** | **security-association lifetime** {**gigabytes** | **kilobytes** | **megabytes** | **seconds**} | **transform-set**}

Syntax Description

peer	Specifies an allowed encryption/decryption peer.
ip-address	Specifies a static IP address for the destination peer.
auto-peer	Specifies automatic assignment of the address for the destination peer.
pfs	Specifies the perfect forwarding secrecy.
group1	(Optional) Specifies PFS DH Group1 (768-bit MODP).
group14	(Optional) Specifies PFS DH Group14 (2048-bit MODP).
group2	(Optional) Specifies PFS DH Group2 (1024-bit MODP).
group5	(Optional) Specifies PFS DH Group5 (1536-bit MODP).
security-association lifetime	Specifies the security association lifetime in traffic volume or time in seconds.
gigabytes *number*	Specifies a volume-based key duration in gigabytes. The range is 1 to 4095.
kilobytes *number*	Specifies a volume-based key duration in kilobytes. The range is 2560 to 2147483647.
megabytes *number*	Specifies a volume-based key duration in megabytes. The range is 3 to 4193280.
seconds *number*	Specifies a time-based key duration in seconds. The range is 600 to 86400.
transform-set	Configures the transform set name or set name list.
set-name	Specifies a transform set name. Maximum length is 63 characters.
set-name-list	Specifies a comma-separated transform set name list. Maximum length of each name is 63 characters. You can specified a maximum of six lists.

Command Default

None.

PFS is disabled by default. When it is enabled without a group parameter, the default is group1.

The security association lifetime defaults to global setting configured by the **crypto global domain ipsec security-association lifetime** command.

Command Modes

IPsec crypto map configuration submode

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

To use this command, IPsec must be enabled using the **crypto ipsec enable** command.

Examples

The following example shows how to configure IPsec crypto map attributes:

```
switch# config terminal
switch(config)# crypto map domain ipsec x 1
switch(config-crypto-map-ip)# set peer auto-peer
```

Related Commands

Command	Description
crypto global domain ipsec security-association lifetime	Configures the global security association lifetime value.
crypto ipsec enable	Enables IPsec.
show crypto map domain ipsec	Displays IPsec crypto map information.

set interface preference-strict (fcroute-map configuration submode)

To configure a Fibre Channel or PortChannel interface strictly by preference level, use the **set interface preference-strict** command. To remove the configuration, use the **no** form of the command.

set interface preference-strict
no set interface preference-strict

Syntax Description

This command has no arguments or keywords.

Command Default

The **set interface preference-strict** default setting is disabled.

Command Modes

Fibre Channel route-map configuration submode.

Command History

Release	Modification
3.0(3)	This command was introduced.

Usage Guidelines

None.

Examples

The following example specifies an interface with a strict preference level.

```
switch# config terminal
switch(config)#
switch(config)# fcroute-map vsan 2 12
switch(config-fcroute-map)# set interface preference-strict
```

The following example removes the strict preference level from an interface.

```
switch(config-fcroute-map)# no set interface preference-strict
```

Related Commands

Command	Description
fcroute	Specifies Fibre Channel routes and activates policy routing.
fcroute-map vsan	Specifies a preferred path Fibre Channel route-map.
show fcroute-map	Displays Fibre Channel route-maps.
match (fcroute-map configuration submode)	Specifies the source and destination FC ID match criteria.
set (fcroute-map configuration submode)	Specifies the interface, the preference level for this interface, and the IVR next hop VSAN ID for this interface.

setup

To enter the switch setup mode, use the **setup** command in EXEC mode.

setup

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The setup utility guides you through the basic configuration process. Type **Ctrl-c** at any prompt to skip the remaining configuration options and proceed with what is configured to that point.

If you do not want to answer a previously configured question, or if you want to skip answers to any questions, press **Enter**. If a default answer is not available (for example switch name), the switch uses what is already configured, and skips to the next question.

Examples

The following example shows how to enter switch setup mode:

```
switch# setup
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup always assumes a predefined defaults irrespective
of the current system configuration when invoked from CLI.
Press Enter incase you want to skip any dialog. Use ctrl-c at anytime
to skip away remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
```

setup ficon

To enter the automated FICON setup mode, use the **setup ficon** command in EXEC mode.

setup ficon

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The setup utility guides you through the basic configuration process. Type **Ctrl-c** at any prompt to skip the remaining configuration options and proceed with what is configured to that point.

If you do not want to answer a previously configured question, or if you want to skip the answers to any questions, press **Enter**. If a default answer is not available (for example switch name), the switch uses what is already configured, and skips to the next question.

Examples

The following example shows how to enter switch setup mode:

```
switch# setup ficon
---- Basic System Configuration Dialog ----
--- Ficon Configuration Dialog ---
This setup utility will guide you through basic Ficon Configuration
on the system.
Press Enter if you want to skip any dialog. Use ctrl-c at anytime
to skip all remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
```

setup sme

To run the basic SME setup facility, use the **setup sme** command.

setup sme

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

Use the **setup sme** command to create the sme-admin and sme-recovery roles for Cisco SME.

Examples

The following example creates the sme-admin and sme-recovery roles:

```
switch# setup sme
Set up two roles necessary for SME, sme-admin and sme-recovery? (yes/no) [no] y
SME setup done
```

Related Commands

Command	Description
show role	Displays information about the various Cisco SME role configurations.

shared-keymode

To configure the shared key mode, use the **shared-keymode** command. To specify the unique key mode, use the **no** form of the command.

shared-keymode
no shared-keymode

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

The **shared-keymode** command generates a single key that is used for a group of backup tapes.

The **no shared-keymode** generates unique or specific keys for each tape cartridge.

Note The shared unique key mode should be specified if you want to enable the key-ontape feature.

Examples

The following example specifies the shared key mode:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# shared-keymode
```

The following example specifies the shared unique keymode:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# no shared-keymode
```

Related Commands

Command	Description
show sme cluster	Displays Cisco SME cluster information.

shutdown

To disable an interface, use the **shutdown** command. To enable an interface, use the **no** form of the command.

shutdown [**force**]
no shutdown [**force**]

Syntax Description

force	(Optional) Forces the shutdown of the mgmt 0 interface without a prompt message.

Command Default

All interfaces are shutdown by default except the mgmt0 interface.

Command Modes

Interface configuration submode

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

When you try to shut down a management interface (mgmt0), a followup prompt message confirms your action before performing the operation. Use the **force** option to bypass this confirmation, if required.

Examples

The following example shows how to enable an interface:

```
switch# config terminal
switch(config)# interface fc 1/2
switch(config-if)# no shutdown
```

The following example shows how to disable an interface:

```
switch# config terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown
Shutting down this interface will drop all telnet sessions.
Do you wish to continue (y/n)? y
```

The following example shows how to forcefully disable the mgmt 0 interface:

```
switch# config terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown force
```

Related Commands

Command	Description
interface	Specifies an interface and enters interface configuration submode.
show interface	Displays interface information.
system default switchport	Configures port attributes.

shutdown (Cisco SME and IOA cluster configuration submode)

To disable a cluster for recovery, use the **shutdown** command. To enable the cluster for recovery, use the **no** form of the command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

SME and IOA clusters are shutdown.

Command Modes

Cisco SME and IOA cluster configuration submode

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

To disable operation of a cluster for the purpose of recovery, use the shutdown command. To enable the cluster for normal usage, use the no shutdown command.

The default state for clusters is no shutdown. Use the shutdown command for cluster recovery.

Examples

The following example restarts the cluster after recovery is complete:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# no shutdown
```

The following example disables the SME cluster operation in order to start recovery:

```
switch# config t
switch(config))# sme cluster c1
switch(config-sme-cl)# shutdown
```

The following example disables the IOA cluster operation:

```
switch# config t
switch(config))# ioa cluster c1
switch(config-ioa-cl)# shutdown
```

Related Commands

Command	Description
show ioa cluster	Displays information about the Cisco IOA cluster.
show sme cluster	Displays information about the Cisco SME cluster.

shutdown (interface configuration submode)

To disable an Cisco SME interface, use the **shutdown** command. To enable the interface, use the **no** form of the command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Interface configuration submode

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

The default state for Cisco SME interfaces is shutdown. Use the no shutdown command to enable the interface to carry traffic.

The show interface command shows that the Cisco SME interface is down until the interface is added to a cluster.

Examples

The following example enables a Cisco SME interface:

```
switch# config t
switch(config)# interface sme 4/1
switch(config-if)# no shutdown
```

The following example disables a Cisco SME interface:

```
switch# config t
switch(config)# interface sme 4/1
switch(config-if)# shutdown
```

Related Commands

Command	Description
show interface sme	Displays information about the Cisco SME interface.

site-id

To configure the site ID with the Call Home function, use the **site-id** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

site-id *site-number*
no site-id *site-number*

Syntax Description

site-number	Identifies the unit to the outsourced throughput. Allows up to 256 alphanumeric characters in free format.

Command Default

None.

Command Modes

Call Home configuration submode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the site ID in the Call Home configuration:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# site-id Site1ManhattanNY
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

sleep

To delay an action by a specified number of seconds, use the **sleep** command.

sleep *seconds*

Syntax Description

seconds	Specifies the delay in number of seconds. The range is 0 to 2147483647.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is useful within scripts.

Examples

The following example shows how to create a script called test-script:

```
switch# show file slot0:test-script
discover scsi-target remote
sleep 10
show scsi-target disk
switch# run-script slot0:test-script
```

When you execute the slot0:test-script, the switch executes the **discover scsi-target remote** command, and then waits for 10 seconds before executing the **show scsi-target disk** command.

The following example shows how to delay the switch prompt return:

```
switch# sleep 30
```

You will see the switch prompt return after 30 seconds.

sme

To enable or disable the Cisco SME services, use the **sme** command.

sme { **cluster** *name* | **transport ssl trustpoint** *trustpoint label* }

Syntax Description

cluster	Configures the cluster.
name	Identifies the cluster name.
transport	Configures the transport information.
ssl	Configures the transport SSL information.
trustpoint	Configures the transport SSL trustpoint.
trustpoint label	Identifies the trustpoint label.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
3.2(2c)	This command was introduced.

Usage Guidelines

Cisco SME services must be enabled to take advantage of the encryption and security features.

To use this command, you must enable Cisco SME clustering using the feature cluster command.

Examples

The following example shows how to configure a cluster:

```
switch# config t
sw-sme-n1(config)# sme cluster clustername
sw-sme-n1(config-sme-cl)#
```

snmp port

Use the **snmp port** command to enable SNMP control of FICON configurations. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

snmp port control
no snmp port control

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP control of FICON configurations is enabled.

Command Modes

FICON configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

By default, SNMP users can configure FICON parameters through the Fabric Manager application. You can prohibit this access, if required, by using the **no snmp port control** command.

Examples

The following example prohibits SNMP users from configuring FICON parameters:

```
switch(config)# ficon vsan 2
switch(config-ficon)# no
 snmp port control
```

The following example allows SNMP users to configure FICON parameters (default):

```
switch(config-ficon)# snmp port control
```

Related Commands

Command	Description
ficon vsan *vsan-id*	Enables FICON on the specified VSAN.
show ficon	Displays configured FICON details.

snmp-server

To configure the SNMP server information, switch location, and switch name, use the**snmp-server** command **in configuration mode.** To remove the system contact information, use the **no** form of the command.

snmp-server {**community** *string* [**group** *group-name* | **ro** | **rw**] | **contact** [*name*] | **location** [*location*]}
no snmp-server {**community** *string* [**group** *group-name* | **ro** | **rw**] | **contact** [*name*] | **location** [*location*]}

Syntax Description

community *string*	Specifies SNMP community string. Maximum length is 32 characters.
group *group-name*	(Optional) Specifies group name to which the community belongs. Maximum length is 32 characters.
ro	(Optional) Sets read-only access with this community string.
rw	(Optional) Sets read-write access with this community string.
contact	Configures system contact.
name	(Optional) Specifies the name of the contact. Maximum length is 80 characters.
location	Configures system location.
location	(Optional) Specifies system location. Maximum length is 80 characters.

Command Default

The default community access is read-only (**ro**).

Command Modes

Configuration mode

Command History

Release	Modification
1.0(3)	This command was introduced.
2.0(1b)	Added **group** option.

Usage Guidelines

None.

Examples

The following example sets the contact information, switch location, and switch name:

```
switch# config terminal
switch(config)# snmp-server contact NewUser
switch(config)# no snmp-server contact NewUser
switch(config)# snmp-server location SanJose
switch(config)# no snmp-server location SanJose
```

Related Commands

Command	Description
show snmp	Displays SNMP information.

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 in configuration mode. To revert to the default settings, use the **no** form of the command.

snmp-server aaa-user cache-timeout *seconds*
no snmp-server aaa-user cache-timeout *seconds*

Syntax Description

seconds	Timeout value, in seconds. The range is from 1 to 86400. The default is 60000.

Command Default

60000 seconds

Command Modes

Global configuration mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example shows how to configure the AAA user synchronization timeout value:

```
switch# config terminal
switch(config)# snmp-server aaa-user cache-timeout 6000
```

Related Commands

Command	Description
show snmp	Displays information about SNMP.

snmp-server aaa exclusive-behavior enable

To enable AAA exclusive behavior on the SNMP server, use the **snmp-server aa exclusive-behavior enable** command in configuration mode. To disable the exclusive behavior command, use the **no** form of the command.

snmp-server aaa exclusive-behavior enable
no snmp-server aaa exclusive-behavior enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

This command when configured will make enable exclusive behavior between local users and aaa users.

- if testuser is local user and if aaa is on, then the queries for testuser will fail saying no such user.
- If testuser2 is aaa user and if aaa is off, then the queries for testuser2 will fail saying no such user.
- If testuser3 is used in both local and aaa user, then if aaa is on then queries with remote credentials succeed and queries with local credential fail saying incorrect password. If aaa is off then queries with local remote credentials succeed and queries with remote credential fail saying incorrect password.

Examples

The following example shows how to enable the aaa exclusive behavior:

```
switch# config t
switch(config)# snmp-server aaa exclusive-behavior enable
switch(config)#
```

The following example shows how to disable the aaa exclusive behavior:

```
switch(config)# no snmp-server aaa exclusive-behavior enable
switch(config)#
```

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server community

To set the SNMP server community string, use the**snmp-server community** command **in configuration mode.** To remove the SNMP server community string, use the **no** form of the command.

snmp-server community *string* [**group** *group-name*]
no snmp-server community *string* [**group** *group-name*]

Syntax Description

community *string*	SNMP community string.
group *group-name*	(Optional) Group to which the community belongs.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets the SNMP server community string:

```
switch# config t
switch(config)# snmp-server community public group network-operator
switch(config)#
switch(config)# no snmp-server community public group network-operator
switch(config)#
```

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server contact

To modify server contact, use the **snmp-server contact** command **in configuration mode.** To remove the SNMP server contact, use the **no** form of the command.

snmp-server contact *line*
no snmp-server contact *line*

Syntax Description

line	(Optional) Modifies the system contact.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to modify the server contact:

```
switch# config t
switch(config)# snmp-server contact line
switch(config)#
switch(config)# no snmp-server contact line
switch(config)#
```

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server enable traps

To enable SNMP server notifications (informs and traps), use the **snmp-server enable traps** command**.** To disable the SNMP server notifications, use the **no** form of the command.

snmp-server enable traps [**entity** [**fru**] | **fcc** | **fcdomain** | **fcns** | **fdmi** | **fspf** | **license** | **link** [**cisco**] | **ietf** [**cisco**] | **ietf-extended** [**cisco**] | **port-security** | **rscn** [**els** | **ils**] | **snmp** [**authentication**] | **vrrp** | **zone** [**default-zone-behavior-change** | **merge-failure** | **merge-success** | **request-reject**]]
no snmp-server enable traps [**entity** [**fru**] | **fcc** | **fcdomain** | **fcns** | **fdmi** | **fspf** | **license** | **link** [**cisco**] | **ietf** [**cisco**] | **ietf-extended** [**cisco**] | **port-security** | **rscn** [**els** | **ils**] | **snmp** [**authentication**] | **vrrp** | **zone** [**default-zone-behavior-change** | **merge-failure** | **merge-success** | **request-reject**]]

Syntax Description

entity	(Optional) Enables all SNMP entity notifications.
fru	(Optional) Enables only SNMP entity FRU notifications.
fcc	(Optional) Enables SNMP Fibre Channel congestion control notifications.
fcdomain	(Optional) Enables SNMP Fibre Channel domain notifications.
fcns	(Optional) Enables SNMP Fibre Channel name server notifications.
fdmi	(Optional) Enables SNMP Fabric Device Management Interface notifications.
fspf	(Optional) Enables SNMP Fabric Shortest Path First notifications.
license	(Optional) Enables SNMP license manager notifications.
link	(Optional) Enables SNMP link traps.
cisco	(Optional) Enables Cisco cieLinkUp/cieLinkDown.
ietf	(Optional) Enables standard linkUp/linkDown trap.
ietf-extended	(Optional) Enables standard linkUp/linkDown trap with extra varbinds.
port-security	(Optional) Enables SNMP port security notifications.
rscn	(Optional) Enables all SNMP Registered State Change Notification notifications.
els	(Optional) Enables only SNMP RSCN ELS notifications.
ils	(Optional) Enables only SNMP RSCN ILS notifications.
snmp	(Optional) Enables all SNMP agent notifications.
authentication	(Optional) Enables only SNMP agent authentication notifications.
vrrp	(Optional) Enables SNMP Virtual Router Redundancy Protocol notifications.
zone	(Optional) Enables all SNMP zone notifications.

default-zone-behavior-change	(Optional) Enables only SNMP zone default zone behavior change notifications.
merge-failure	(Optional) Enables only SNMP zone merge failure notifications.
merge-success	(Optional) Enables only SNMP zone merge success notifications.
request-reject	(Optional) Enables only SNMP zone request reject notifications.

Command Default

All the notifications listed in the Syntax Description table are disabled by default except for the following: **entity fru**, **vrrp**, **license**, **link**, and any notification not listed (including the generic notifications such as **coldstart**, **warmstart**, and **linkupdown**).

Command Modes

Configuration mode

Command History

Release	Modification
2.0(1b)	This command was introduced.
2.1(2)	• Added the link option. • Renamed the **standard** option to **ietf**. • Renamed the **standard-extended** option to **ietf-extended**.

Usage Guidelines

If the **snmp-server enable traps** command is entered without keywords, all notifications (informs and traps) are enabled.

As of Cisco MDS SAN-OS Release 2.1(2), you can configure the linkUp/linkDown notifications that you want to enable on the interfaces. You can enable the following types of linkUp/linkDown notifications:

- Cisco—Only traps (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface.
- IETF—Only traps (linkUp, linkDown) defined in IF-MIB are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Only the varbinds defined in the trap definition are sent with the traps.
- IETF extended—Only traps (linkUp, linkDown) defined in IF-MIB are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. In addition to the varbinds defined in the trap definition, varbinds defined in the IF-MIB specific to the Cisco Systems implementation are sent. This is the default setting.
- IETF cisco—Traps (linkUp, linkDown) defined in IF-MIB and traps (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Only the varbinds defined in the trap definition are sent with the linkUp and linkDown traps.
- IETF extended cisco—Traps (linkUp, linkDown) defined in IF-MIB and traps (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. In addition to the varbinds defined in the linkUp and linkDown trap definition, varbinds defined in the IF-MIB specific to the Cisco Systems implementation are sent with the linkUp and linkDown traps.

Examples

The following example enables all the SNMP notifications listed in the Syntax Description table:

```
switch# config terminal
switch(config)# snmp-server traps
```

The following example enables all SNMP entity notifications:

```
switch# config terminal
switch(config)# snmp-server traps entity
```

The following example enables (default) only standard extended linkUp/linkDown notifications:

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

The following example enables only Cisco Systems defined cieLinkUp/cieLinkDown notifications:

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

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server host	Configures SNMP server host information.

snmp-server enable traps fcdomain

To enable SNMP FC domain traps, use the**snmp-server enable traps fcdomain** command **in configuration mode.** To disable FC domain trap, use the **no** form of the command.

snmp-server enable traps fcdomain
no snmp-server enable traps fcdomain

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification trap
4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable SNMP FC domain traps:

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

Related Commands

Command	Description
show snmp	Displays SNMP information.
show snmp trap	Displays SNMP traps.

snmp-server enable traps link cisco

To enable Cisco cieLinkUp and cieLinkDown traps, use the**snmp-server enable traps link cisco** command **in configuration mode.** To disable Cisco link trap, use the **no** form of the command.

snmp-server enable traps link cisco
no snmp-server enable traps link cisco

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification trap
4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable SNMP FC domain traps:

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

Related Commands

Command	Description
show snmp	Displays SNMP information.
show snmp trap	Displays SNMP traps.

snmp-server enable traps zone

To enable SNMP zone traps, use the **snmp-server enable traps zone** command **in configuration mode.** To disable zone trap, use the **no** form of the command.

snmp-server enable traps zone
no snmp-server enable traps zone

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification trap
4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable SNMP zone traps:

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

Related Commands

Command	Description
show snmp	Displays SNMP information.
show snmp trap	Displays SNMP traps.

snmp-server globalEnforcePriv

To globally enforce privacy for all SNMP users, use the **snmp-server globalEnforcePriv** command in configuration mode. To disable global privacy, use the **no** form of the command.

snmp-server globalEnforcePriv
no snmp-server globalEnforcePriv

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
2.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables globally enforced privacy for all SNMP users:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server globalEnforcePriv
```

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server host

To specify the recipient of an SNMP notification, use the **snmp-server host** global configuration command. To remove the specified host, use the **no** form of the command.

snmp-server host {*ipv4-addressipv6-addressdns-name*} [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*]
no snmp-server host {*ipv4-addressipv6-addressdns-name*} [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*]

Syntax Description

ipv4-address	Specifies the IPv4 address of the host (the targeted recipient).
ipv6-address	Specifies the IPv6 address of the host (the targeted recipient).
dns-name	Specifies the DNS server name of the host (the targeted recipient). SNMP hostname using DSN server name starting with 0. or 127. is not supported.
traps	(Optional) Sends SNMP traps to this host.
informs	(Optional) Sends SNMP informs to this host.
version	(Optional) Specifies the version of the Simple Network Management Protocol (SNMP) used to send the traps. Version 3 is the most secure model, as it allows packet encryption with the **priv** keyword.
1	SNMPv1 (default). This option is not available with informs.
2c	SNMPv2C.
3	SNMPv3 has three optional keywords (**auth**, **no auth** (default), or **priv**).
auth	(Optional) Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication
noauth	(Optional) Specifies the noAuthNoPriv security level.
priv	(Optional) Enables Data Encryption Standard (DES) packet encryption (privacy).
community-string	Sends a password-like community string with the notification operation.
udp-port *port*	(Optional) Specifies the port UDP port of the host to use. The default is 162.

Command Default

Sends SNMP traps.

Command Modes

Configuration mode

Command History

Release	Modification
1.0(3)	This command was introduced.

Usage Guidelines

If you use the version keyword, one of the following must be specified: **1**, **2c**, or **3**.

Examples

The following example specify the recipient of an SNMP notification:

```
switch# config terminal
switch(config)# snmp-server host 10.1.1.1 traps version 2c abcddsfsf udp-port 500
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server host	Configures SNMP server host information.

snmp-server location

To modify system location, use **snmp-server** location command. To remove the SNMP server location, use the **no** form of the command.

snmp-server location
no snmp-server location

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets the SNMP server community string:

```
switch# config t
switch(config)# snmp-server location line
switch(config)#
```

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server tcp-session

To enable one time authentication for SNMP over a TCP session, use the **snmp-server tcp-session** command in configuration mode. To disable one time authentication for SNMP over a TCP session, use the **no** form of the command.

snmp-server tcp-session [**auth**]
no snmp-server tcp-session [**auth**]

Syntax Description

auth	(Optional) Enables one time authentication for SNMP over a TCP session.

Command Default

One time authentication for SNMP over a TCP session is on.

Command Modes

Configuration mode

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables one time authentication for SNMP over a TCP session:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server tcp-session auth
```

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server traps entity fru

To enable SNMP entity FRU trap, use the **snmp-server traps entity fru** command **in configuration mode.** To disable entity FRU trap, use the **no** form of the command.

snmp-server enable traps entity fru
no snmp-server enable traps entity fru

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification trap
4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable SNMP entity FRU trap:

```
switch# config t
switch(config)# snmp-server enable traps entity fru
switch(config)#
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
show snmp trap	Displays SNMP traps.

snmp-server user

To configure SNMP user information, use the **snmp-server user** commandin **configuration mode.** To disable the configuration or to revert to factory defaults, use the **no** form of the command.

snmp-server user *username group-name* [**auth** {**md5** | **sha**} *password* [**priv** [*password* [**auto** | **localizedkey** [**auto**]]] | **aes-128** *password* [**auto** | **localizedkey** [**auto**] | **auto** | **localizedkey** [**auto**]]]]
no snmp-server user *name* [*group-name* | **auth** {**md5** | **sha**} *password* [**priv** [*password* [**auto** | **localizedkey** [**auto**]]] | **aes-128** *password* [**auto** | **localizedkey** [**auto**] | **auto** | **localizedkey** [**auto**]]]]

Syntax Description

username	Specifies the user name. Maximum length is 32 characters.
group-name	(Optional) Specifies role group to which the user belongs. Maximum length is 32 characters.
auth	(Optional) Sets authentication parameters for the user.
md5	Sets HMAC MD5 algorithm for authentication.
sha	Uses HMAC SHA algorithm for authentication.
password	(Optional) Specifies user password. Maximum length is 64 characters.
priv	(Optional) Sets encryption parameters for the user.
auto	(Optional) Specifies whether the user is autocreated (volatile).
localizedkey	(Optional) Sets passwords in localized key format.
aes-128	(Optional) Sets 128-byte AES algorithm for privacy.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
4.2(1)	This command was deprecated.
4.1(1b)	Added engineID options.
1.0(2)	This command was introduced.
1.0(3)	Added the **localizedkey** option.
2.0(1b)	Added the **auto** and **aes128** options.

Usage Guidelines

The localized keys are not portable across devices as they contain information on the engine ID of the device. If a configuration file is copied into the device, the passwords may not be set correctly if the configuration file was generated at a different device. We recommend that passwords be explicitly configured to the desired passwords after copying the configuration into the device.

SNMP Version 3 is the most secure model, as it allows packet encryption with the **priv** keyword.

To assign multiple roles to a user, perform multiple **snmp-server user** *username group-name* commands. The *group-name* argument is defined by the **role name** command.

Examples

The following example sets the 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
```

The following example sets the user information:

```
switch# config terminal
switch(config)# snmp-server user joe network-admin auth sha abcd1234 engineID
switch(config)# snmp-server user sam network-admin auth md5 abcdefgh
switch(config)# snmp-server user Bill network-admin auth sha abcd1234 priv abcdefgh
switch(config)# snmp-server user user1 network-admin auth md5 0xab0211gh priv 0x45abf342
localizedkey
```

Related Commands

Command	Description
role name	Configures role profiles.
show snmp	Displays SNMP information.
snmp-server host	Configures SNMP server host information.

snsr-grp

To link a sensor group to a subscription node and set the data sampling interval, use the **snsr-grp** command. To remove the sensor group, use the **no** form of this command.

snsr-group *id* **sample-interval** *interval*

no snsr-group

Syntax Description

id	Sensor group ID. Range is from 1 to 4095.
sample-interval *interval*	Data sampling interval in milliseconds. Range is from 0 to 604800000.

Command Default

No sensor group exists.

Command Modes

Telemetry subscription configuration mode (conf-tm-sub)

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

Currently, sensor group ID supports only numeric ID values. The interval value is specified by the user and the value is milliseconds. The minimum supported interval is 30000 milliseconds. An interval value greater than the minimum value creates a frequency-based subscription, in which telemetry data is sent periodically at the specified interval.

Examples

This example shows how to link a sensor group to a a subscription node and set the data sampling interval of 30000 milliseconds:

```
switch# configure
switch(config)# telemetry
switch(config-telemetry)# subscription 100
switch(conf-tm-sub)# snsr-grp 100 sample-interval 30000
```

This example shows how to remove the sensor group:

```
switch# configure
switch(config)# telemetry
switch(config-telemetry)# subscription 100
switch(conf-tm-sub)# no snsr-grp 100
```

Related Commands

Command	Description
feature telemetry	Enables the SAN Telemetry Streaming feature.

Command	Description
sensor-group	Creates a sensor group and enters sensor group configuration.
show running-config telemetry	Displays the existing telemetry configuration.
show telemetry	Displays telemetry configuration.
subscription	Creates a subscription node and enters subscription node configuration mode.
telemetry	Enters SAN Telemetry Streaming configuration mode.

source

To configure the SPAN session source, use the **source** command in Configuration mode. To revert to the default settings, use the **no** form of this command.

source { **filter vsan** *vsan-id* | **interface ethernetsource** | **ethernet-port-channel** | **fc** *module-number* | **port-channel** *port-channel-number* | **sup-eth** | **sup-fc** *inband interface number* | **vlan** *vlan-id* | **vsan** *vsan-id*}
{**no source filter vsan** *vsan-id* | **interface ethernet** | **ethernet-port-channel** | **fc** *module-number* | **port-channel** *port-channel-number* | **sup-eth** | **sup-fc** *inband interface number* | **vlan** *vlan-id* | **vsan** *vsan-id*}

Syntax Description

filter	Configures SPAN session filter.
vsan	Specifies the VSAN.
vsan-id	Specifies the VSAN ID. The range is from 1 to 4093
interface	Specifies the interface type.
ethernet	Specifies the ethernet.
ethernet-port-channel	Specifies the ethernet port channel interface.
fc	Specifies Fibre channel interface.
module-number	Specifies the module number. The range is from 1 to 10.
port-channel	Specifies the port channel interface.
port-channel-number	Specifies the port channel number. The range is from 1 to 256.
sup-eth	Specifies the ethernet inband interface.
sup-fc	Specifies the fibre channel inband interface.
inband interface number	Specifies the inband interface. The range is from 0 to 0.
vlan	Specifies the VLAN.
vlan-id	Specifies the VLAN ID. The range is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	Added the keywords ethernet, ethernet-port-channel, sup-eth,vlan to the syntax description.

Usage Guidelines

None.

Examples

The following example shows how to configure the SPAN traffic in ingress, egress and both directions:

```
switch# config
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# monitor session 1
switch(config-monitor)# source interface fc 1/5 rx
switch(config-monitor)# source interface fc 1/5 tx
switch(config-monitor)# source interface fc 1/5 both
switch(config-monitor)# destination interface fc 1/5
```

Related Commands

Command	Description
show monitor session all	Displays all information about the Switched Port Analyzer (SPAN) session.

span max-queued-packets

To configure the SPAN max-queued-packets, use the **span max-queued-packets** command in configuration mode. To disable the SPAN drop-threshold, use the **no** form of the command.

span max-queued-packets *id*
no span max-queued-packets *id*

Syntax Description

id	Specifies the SPAN max-queued-packets threshold ID. The range is 1 to 8191.

Command Default

15.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

This command is supported only on a ISOLA platform.

Examples

The following example shows how to configure the SPAN max-queued-packets:

```
switch# config
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# span max-queued-packets 1
```

Related Commands

Command	Description
show span drop-counters	Displays the SPAN drop-counters.
show span max-queued-packets	Displays the SPAN max-queued-packets.

span session

To configure a SPAN session, use the **span session** command. To remove a configured SPAN feature or revert it to factory defaults, use the **no** form of the command.

span session *session-id* {**destination** | **filter** | **no** | **rate-optional** | **source** | **suspend**}
no span session *session-id* {**destination** | **filter** | **no** | **rate-optional** | **source** | **suspend**}

Syntax Description

session-id	Specifies the SPAN session ID. The range is 1 to 16.
destination	Specifies the destination configuration.
filter	Specifies the filter configuration.
no	Specifies the default value.
rate-optional	Specifies the rate limit for SPAN packets on FCOE module. IS there a variable associated with this? Does this have a range.
source	Specifies the source configuration.
suspend	Specifies the SPAN suspended session.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure a SPAN session:

```
switch# config terminal
switch(config)# span session 1
switch(config-span)#
```

The following example shows how to delete a SPAN session:

```
switch(config)# no
 span session 1
```

Related Commands

Command	Description
destination interface	Configures a SPAN destination interface.
show span session	Displays specific information about a SPAN session.
source	Configures a SPAN source.
span session	Selects or configures the SPAN session and changes to SPAN configuration submode.
suspend	Suspends a SPAN session.
switchport	Configures the switch port mode on the Fibre Channel interface.

span session source interface

To configure the SPAN traffic in both ingress (rx) and egress (tx) directions, use the **span sessionsourceinterface** command in Configuration mode. To revert this command. use the **no** form of this command.

interface

span session*session-id***source interface** *interface type*
no span session *session-id* **source interface** *interface type*

Syntax Description

session-id	Specifies the SPAN session ID.
interfacetype	Specifies the destination interface mapped to a Fiber Channel or FC tunnel.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
1.0(x)	This command was introduced.
3.3(1a)	Enabled SPAN traffic in both ingress (rx) and egress (tx) directions for Generation 2 Fabric Switches.

Usage Guidelines

None.

Examples

The following example shows how to configure the SPAN traffic in both ingress and egress directions:

```
switch# config
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# span session 1
switch(config-span)# source interface fc 1/5 rx
switch(config-span)# source interface fc 1/5 tx
switch(config-span)# destination interface fc 1/5
```

Related Commands

Command	Description
show span session	Displays specific information about a Switched Port Analyzer (SPAN) session.

special-frame

To enable or disable special frames for the FCIP interface, use the **special-frame** command. To disable the passive mode for the FCIP interface, use the **no** form of the command.

special-frame peer-wwn *pwwn-id* [**profile-id** *profile-number*]
no special-frame peer-wwn *pwwn-id*

Syntax Description

peer-wwn *pwwn-id*	Specifies the peer WWN ID for special frames.
profile-id *profile-number*	(Optional) Specifies the peer profile ID. The range is 1 to 255.

Command Default

Disabled.

Command Modes

Interface configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the switch(config-if)# submode.

When a new TCP connection is established, an FCIP special frame (if enabled) makes one round trip from the FCIP profile and initiates the TCP connect operation to the FCIP profile receiving the TCP connect request and back. Use these frames to identify the FCIP link endpoints, to learn about the critical parameters shared by Fibre Channel and FCIP profile pairs involved in the FCIP link, and to perform configuration discovery.

Examples

The following example configures the special frames:

```
switch# config terminal
switch(config)# interface fcip 1
switch(config)# special-frame peer-pwwn 11:11:11:11:11:11:11:11
switch(config)# special-frame peer-pwwn 22:22:22:22:22:22:22:22 profile-id 10
```

Related Commands

Command	Description
show interface fcip	Displays an interface configuration for a specified FCIP interface.

ssh

To initiate a Secure Shell (SSH) session, use the **ssh** command in EXEC mode.

ssh { **hostname** | **userid@hostname** }

Syntax Description

hostname	Specifies the name or IP address of the host to access.
userid @ hostname	Specifies a user name on a host.

Command Default

The default user name is admin.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to initiate an SSH session using a host name:

```
switch# ssh host1
admin@1host1's password:
```

The following example shows how to initiate an SSH session using a host IP address:

```
switch# ssh 10.2.2.2
admin@10.1.1.1's password:
```

The following example shows how to initiate an SSH session using a user name host name:

```
switch# ssh user1@host1
user1@1host1's password:
```



Note The ssh command supports only AES-CTR ciphers from version 5.2(8g) and version 6.2(13) onwards, because the other ciphers are considered to be weak by Federal Information Processing Standards (FIPS).



Note To discover the fabric in DCNM with 5.2(8g) and 6.2(13) images, you must install DCNM 7.1(2); as it supports the AES-CTR ciphers.

Related Commands

Command	Description
feature ssh	Enables SSH server.
show ssh key	Displays SSH key information.

ssh {ciphers | macs | keytypes | kexalgos| cipher-mode | login-attempts |login-gracetime |rekey } all

To enable SSH key exchange algorithms, message authentication codes (MACs), key types, and ciphers to encrypt the connections, use the **ssh {ciphers | macs | keytypes | kexalgos| cipher-mode| login-attempts| login-gracetime| rekey} all** command in configuration mode. Use the **no** form of this command to disable weak ciphers.

ssh { **ciphers** | **macs** | **keytypes** | **kexalgos** | **cipher-mode** | **login-attempts** | **login-gracetime** | **rekey** } { **WORD** | **all** }

no ssh { **ciphers** | **macs** | **keytypes** | **kexalgos** | **cipher-mode** | **login-attempts** | **login-gracetime** | **rekey** }

Syntax Description

ciphers	Specifies ciphers to encrypt the connection
macs	Specifies message authentication codes used to detect traffic modification
keytypes	Specifies public key algorithms that the server can use to authenticate itself to the client
kexalgos	Specifies the key exchange methods that are used to generate per-connection keys
WORD	Specify the name of the algorithm to be configured.
all	Includes all known weak SSH algorithms in current version of NX-OS in addition to the base set of strong algorithms
cipher-mode	Set Cipher-mode for ssh
login-attempts*value*	Set maximum login attempts. Enter value in range <1 to 10>
login-gracetime*time*	Set login gracetime for ssh connection. Enter in seconds
rekey*data sizetime*	Renegotiate ssh key.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
9.4(1)	This command was introduced.

Usage Guidelines

Supported Ciphers with ssh ciphers all command are:

- aes128-cbc
- aes192-cbc
- aes256-cbc

- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes256-gcm@openssh.com
- aes128-gcm@openssh.com

Supported MACs with ssh macs all command are:

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512

Supported types of public key cryptography with ssh keytypes all command are:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-dss
- ssh-rsa

Supported Key Exchange Algorithms with ssh kexalgos all are:

- curve25519-sha256
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

Example

The following example shows how to enable all supported ciphers to encrypt the connection:

```
switch# configure terminal
switch(config)# ssh ciphers all
switch(config)#
```

Example

The following example shows how to enable all supported MACs which are the message authentication codes used to detect traffic modification.

```
switch# configure terminal
switch(config)# ssh macs all
switch(config)#
```

Example

The following example shows how to enable all supported public key algorithms.

```
switch# configure terminal
switch(config)# ssh keytypes all
switch(config)#
```



Note To enable rsa, dsa and ecdsa key types corresponding SSH host keys should be generated.

Example:

- `ssh key dsa`
- `ssh key rsa 2048`
- `ssh key ecdsa 521`

Example

The following example shows how to enable all supported KexAlgorithms which are the key exchange methods that are used to generate per-connection keys.

```
switch# configure terminal
switch(config)# ssh kexalgos all
switch(config)#
```

ssh connect

To log in to a destination using a channel of previously established SSH session, use the **ssh connect** command.

ssh connect *label*

Syntax Description

label	Handle of an already established SSH session.

Command Default

No sessions are defined.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

Enable **feature ssh** and configure the **ssh name** command before executing the **ssh connect** command.

The following example shows how to connect to a destination over SSH with a local name of 'me@host'. This name has already been configured using the **ssh name** command.

```
switch# ssh connect me@host
host$
```

Related Commands

Command	Description
ssh name	Opens an SSH session to a destination and apply label to it.
sscp	Redirects the output using streaming secure copy (sscp) to a named SSH connection.
show ssh names	Displays all shareable SSH sessions established on the switch.

ssh idle-timeout

Use the **ssh idle-timeout** command to control the duration an SSH client session connected to the switch can remain idle before being closed by NX-OS.

If the remote SSH client does not send any packets to the switch for the timeout period then the session is timed out. If the keepalive count is enabled the switch sends a keepalive packet to the remote SSH client. If the client responds the session is kept and the timeout and keepalive count are reset. If the keepalive response does not reach the switch the timeout and keepalive sequence is repeated up to the configured count. If no response is received for all the keepalive packets the session is closed.

ssh idle-timeout *time* [**keepalive-count** *count*]

no ssh idle-timeout

Syntax Description

keepalive-count *count*	(Optional) Maximum count of keepalive packets to be sent to the SSH client. 0 to disable. Default is 0.
time	Idle timeout period in seconds. 0 to disable. Default is 0.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
9.4(1)	This command was introduced.

Usage Guidelines

This command applies to SSH sessions created after it is executed. Existing sessions use the configuration at the time they were created.

Examples

The following example configures the SSH client session idle timeout to 300 seconds and the keepalive count to three tries. This equates to 300 x 3 = 900 seconds of no packets received from the SSH client before the session is closed.

```
switch# configure terminal
switch(config)# feature ssh
switch (config)# ssh idle-timeout 300 keepalive-count 3
```

Related Commands

Command	Description
feature ssh	Enables SSH server.
show accounting log	Displays user login history.
show users	Displays currently connected sessions and idle time.

ssh key

To generate an SSH key, use the **ssh key** command in configuration mode. To delete SSH keys, use the **no** form of the command.

ssh key {**dsa** | **rsa** [*rsa_mod*]} [**force**]
no ssh key [**dsa** | **rsa**]

Syntax Description

dsa	Specifies a DSA key.
rsa	Specifies an RSA key.
rsa_mod	(Optional) The modulus of the RSA key. The range is from 768 to 2048. Starting from Cisco MDS NX-OS Release 8.4(1), the range is from 1024 to 4096.
force	(Optional) Forces the generation of DSA SSH keys even when the keys are present.

Command Default

The default key-pair modulus is 1024 bits.

Command Modes

Configuration mode

Command History

Release	Modification
1.0(2)	This command was introduced.
8.4(1)	The **ssh key rsa** range was modified to 4096 bits.

Usage Guidelines

It is required to disable the SSH service prior to using the **no** form of the command to delete all SSH keys. This, in turn, requires all SSH sessions to be closed. To access the switch without SSH, either log in through the console, or enable Telnet access. Ensure to generate new keys when re-enabling the SSH service. SSH access to the switch will be denied if no SSH keys are installed.

Examples

The following example shows how to generate an RSA key-pair:

```
switch(config)# ssh key rsa 1024
generating rsa key.....
generated rsa key
```

The following example shows how to replace an SSH server key using DSA with the **force** option:

```
switch(config)# no ssh server enable
switch(config)# ssh key dsa force
switch(config)# ssh server enable
```

The following example shows how to delete all SSH key-pairs on the switch:

```
switch(config)# no ssh key
cleared RSA keys
```

Related Commands

Command	Description
feature ssh	Enable or disable SSH service.
show ssh key	Displays SSH key information.

ssh name

To create an SSH session from the switch to a destination for other commands to use, use the **ssh name** command. To close the SSH session, use the **no** form of the command.

ssh name *label user-name destination*

no ssh name *label*

Syntax Description

label	Configures a name of the SSH session.
user-name	Specifies a username to log in to the remote SSH server.
destination	Specifies a domain name or IP address of the remote SSH server.

Command Default

No sessions are defined.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

The **ssh name** command opens an SSH session to the destination as the named user when it is entered. If the user needs to enter a password to log in to the destination then it must be entered at this time. If the user has passwordless SSH configured then no password is required. After authentication, the user is returned to the switch prompt and the SSH session kept open in the background for use by other commands. These subsequent commands do not need to authenticate again with the destination as they use the session opened by this command.

Sessions stay open even after the user who created the sessions logs out. The sessions can be manually closed with the **no** form of the command or will be closed automatically when the supervisor resets (for example, during a supervisor switchover in a dual supervisor system).

This command is not stored in the switch configuration. After a reload, the command configurations are lost and you need to reconfigure the command.

Enable **feature ssh** before configuring the **ssh name** command.

The following example shows how to create an SSH session to destination 192.168.1.1 as user 'ajax', and give it a name of 'me@host' that can be used later by other commands. In the following example, non-passwordless authentication is used:

```
switch# ssh name me@host ajax 192.168.1.1

The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA key fingerprint is SHA256:4VbYNa7hJLPu/4jQEk6Ymn2KU+IMRkrX/miJIEVIP34.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA) to the list of known hosts.
This is a Cisco managed device to be used only for authorized purposes.
Your use is monitored for security, asset protection, and policy compliance.
```

```
Outbound-ReKey for 192.168.1.1
Inbound-ReKey for 192.168.1.1

This is a Cisco managed device to be used only for authorized purposes.
Your use is monitored for security, asset protection, and policy compliance.

me@host @192.168.1.1's password:
```

Related Commands

Command	Description
ssh connect	Initiates an SSH session to a named SSH destination.
sscp	Redirects the output using streaming secure copy (sscp) to a named SSH destination.
show ssh names	Displays all shareable SSH ssessions established on the switch.

ssh server enable

To enable the SSH server, use the **ssh server enable** command in configuration mode. To disable the SSH service, use the **no** form of the command.

ssh server enable
no ssh server enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
1.0(2)	This command was introduced.
8.1(1)	This command was replaced with **feature ssh**.

Usage Guidelines

None.

Examples

The following example enables the SSH server:

```
switch# config terminal
switch(config)# ssh server enable
updated
```

The following example disables the SSH server:

```
switch# config terminal
switch(config)# no
 ssh server enable
updated
```

Related Commands

Command	Description
show ssh server	Displays SSH server information.
ssh key	Generates an SSH key.

ssl

To configure Secure Sockets Layer (SSL), use the **ssl** command. Use the **no** form of this command to disable this feature.

ssl kmc
no ssl kmc

Syntax Description

kmc	Enables SSL for Key Management Center (KMC) communication.

Command Default

None.

Command Modes

Cisco SME cluster configuration mode submode

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables SSL:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# ssl kmc
```

ssm enable feature

To enable a feature on the Storage Services Module (SSM), use the **ssm enable feature** command. To disable the feature on the module, use the **no** form of the command.

ssm enable feature {**dmm** {**force** {**interface fc** *slot-port* | **module slot node slot**} | **interface fc** *slot-port* | **module** *slot* | **invista** {**bootflash:** *uri* | **force module** *slot-number* | **modflash:** *uri* | **module** *slot-number* | **slot0:** *uri*}} | **interface** {**fc** *slot-port-port* | **module** *slot-number* | **force module** *slot-number* | **modflash:** *uri* | **module** *slot-number* | **slot0:** *uri*} | **santap** {**force module** *slot-number* | **interface fc** *slot-port-port* | **module** *slot-number*} | **scsi-flow** {**force module** *slot-number* | **interface fc** *slot-port-port* | **module** *slot-number*}}
no ssm enable feature {**dmm** {**force** {**interface fc** *slot-port* | **module slot node slot**} | **interface fc** *slot-port* | **module** *slot* | **invista** {**bootflash:** *uri* | **force module** *slot-number* | **modflash:** *uri* | **module** *slot-number* | **slot0:** *uri*}} | **interface** {**fc** *slot-port-port* | **module** *slot-number* | **force module** *slot-number* | **modflash:** *uri* | **module** *slot-number* | **slot0:** *uri*} | **santap** {**force module** *slot-number* | **interface fc** *slot-port-port* | **module** *slot-number*} | **scsi-flow** {**force module** *slot-number* | **interface fc** *slot-port-port* | **module** *slot-number*}}

Syntax Description

dmm	Specifies the DMM feature on the SSM.
force	Forces a switching module reload.
interface	Specifies the interface.
fc *slot/port*	Specifies the Fiber Channel slot and port numbers.
node slot	Specifies the node number for partial provisioning of Storage Services Node card. The range is from 0 to 3 characters.
module *slot*	Specifies the SSM module slot number.
invista	Enables the Invista feature on the SSM.
bootflash: *uri*	Specifies the source location for internal bootflash with image name.
force	Forces an immediate configuration change.
module *slot-number*	Specifies the slot number of the SSM.
modflash: uri	Specifies the source location for internal modflash with image name.
slot0:*uri*	Specifies the source location for the CompactFlash memory or PC card with image name.
interface fc *slot*/*port*	Specifies the interface to be configured.
fc *slot*/*port*	Configures the Fibre Channel interface.
fc *slot*/*port-port*	Configures the Fibre Channel interface range of ports. See the Usage Guidelines for this command for a list of interface range restrictions.
santap	Enables the SANTap feature on the SSM.

scsi-flow	Enables the SCSI flow feature on the SSM.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
NX-OS 5.0(1a)	Added node keyword to the syntax description.
3.2(1)	Added dmm keyword to the syntax description.
2.0(2b)	This command was introduced.
2.1(1a)	Added **emcsr, nasb,** and **santap** options.
3.0(1)	Changed the name of the **emcsr** option to **invista**.

Usage Guidelines

Use the **ssm enable feature scsi-flow** command to enable the SCSI flow feature on an SSM.

The features invista and nsp can only be provisioned on a module basis. The features **nasb, santap**, and **scsi-flow** can be provisioned on either a module or a range of interfaces.

The image must be specified when configuring the **invista** and **nsp** features.

Starting with NX-OS 4.1(1b), DMM must be enabled using the ssm enable feature dmm command before using the SLD tool.



Caution The **force** option is only applicable when unprovisioning (using the **no** parameter). Using the **force** parameter without the **no** keyword causes the SSM to reload.

For SAN-OS Release 2.1 and later NX-OS Release 4.1 images, intelligent services can be configured on a range of interfaces with the following restrictions:

- The minimum range is four interfaces.
- The range of interfaces must be specified in multiples of four interfaces. For example, 4, 8, 12, 16, 20, 24, 28, 32.
- Ranges start at the following specific ports: 1, 5, 9, 13, 17, 21, 25, and 29.

Examples

The following example shows how to enable DMM on a module with the node ID which is stored as a part of the key:

```
switch(config)# ssm enable feature dmm module 4 node 2
is node is 0
is force is  0
is node is 0
is force is  0
Got node information
is node is 1
is force is  0
Provisioning failed: Specified module is either not an ILC(SSM/18+4/9222i) or no
```

```
t online yet
switch(config)#
```

The following example shows how to enable DMM on a module:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ssm enable feature dmm module 1
```

The following example shows how to enable DMM on an interface:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ssm enable feature dmm interface fc 1/1 - 4
```

The following example shows how to force a reload on some of the ports on a module:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ssm enable feature dmm force interface fc 1/1 - 8, fc 1/13 - 16
```

The following example enables the Invista feature on the SSM in slot 4:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config) ssm enable feature invista module 4
```

The following example enables the Invista feature using the bootflash image name:

```
switch(config) ssm enable feature invista bootflash:image_name
```

The following example enables the Invista feature using the image name found on the PC card flash module in slot0:

```
switch(config) ssm enable feature invista slot0:image_name
```

The following example disables the Invista feature on the SSM in slot 4:

```
switch(config) no ssm enable feature invista force module 4
```

The following example enables the SANTap feature on the SSM in slot 4:

```
switch(config) ssm enable feature santap module 4
```

The following example enables the SCSI flow feature on the SSM in slot 4:

```
switch(config) ssm enable feature scsi-flow module 4
```

Related Commands

Command	Description
scsi-flow distribute	Configures the SCSI flow services.
show scsi-flow	Displays SCSI flow configuration and status.

ssm upgrade delay

To configure the upgrade delay time, use the **ssm upgrade delay** command. To clear the already set upgrade value, use the **no** form of the command.

ssm upgrade delay *string*
no ssm upgrade delay *string*

Syntax Description

string	Specifies the delayed time in seconds. The range is from 1 to 600.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

During the upgrade, the second SSM and MSM and the subsequent SSMs and MSMs would be delayed by the configured delay value.

Examples

The following example shows how to configure the SSM upgrade delay time:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ssm upgrade delay 500
switch(config)#
```

Related Commands

Command	Description
ssm enable feature	Enables the SCSI flow feature on the SSM.

static (iSCSI initiator configuration and iSLB initiator configuration)

To assign persistent WWNs to an iSCSI initiator or iSLB initiator, use the **static** command in iSCSI initiator configuration submode or iSLB initiator configuration submode. To disable this feature, use the **no** form of the command.

static {**nwwn** | **pwwn**} {*wwn-id* | **system-assign**}
no static {**nwwn** | **pwwn**} {*wwn-id* | **system-assign**}

Syntax Description

nwwn	Configures the initiator node WWN hex value.
pwwn	Configures the peer WWN for special frames.
wwn-id	Specifies the pWWN or nWWN ID.
system-assign	Generates the pWWN or nWWN value automatically.

Command Default

None.

Command Modes

iSCSI initiator configuration submode

iSLB initiator configuration submode

Command History

Release	Modification
1.3(2)	This command was introduced.
3.0(1)	Added iSLB initiator configuration submode.

Usage Guidelines

We recommend using the **system-assign** option. If you manually assign a WWN, you must ensure its uniqueness. You should not use any previously-assigned WWN.

If you use system-assign option to configure WWNs for an iSLB initiator, when the configuration is saved to an ASCII file, the system-assigned WWNs are also saved. If you subsequently perform a write erase, you must manually delete the WWN configuration from the ASCII file. Failing to do so can cause duplicate WWN assignments if the ASCII configuration file is reapplied on the switch.

Examples

The following example uses the switch WWN pool to allocate the nWWN for this iSCSI initiator and to keep it persistent:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# iscsi ?
  authentication  Configure global iscsi authentication parameters
  enable          Enable/Disable iSCSI
  import          Configure import of FC targets to iSCSI domain
```

```
  initiator       Configure iSCSI initiator
  interface       Configure iSCSI interface property
  save-initiator  Make WWNs for initiator persistent
  virtual-target  Configure iSCSI Virtual Target
switch(config)# iscsi initiator ?
  idle-timeout  ISCSI initiator idle timeout value in seconds
  ip-address    ISCSI initiator node ip address
  name          ISCSI initiator node name
switch(config)# iscsi initiator name ?
  <WORD>  Enter Initiator node name (max 223) (Max Size - 223)
switch(config)# iscsi initiator name test ?
  <cr>  Carriage Return
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)# static nWWN system-assign
```

The following example uses the switch WWN pool to allocate two pWWNs for this iSCSI initiator and to keep it persistent:

```
switch(config-iscsi-init)# static pWWN system-assign 2
```

The following example shows a system-assigned pWWN for an iSLB initiator:

```
switch# config t
switch(config)# islb initiator ip-address 209.165.200.226
```

switch(config-islb-init)# static pwwn system-assign 4

The following example removes the system-assigned pWWN for the iSLB initiator:

```
switch (config-islb-init)# no
 static pwwn system-assign 4
```

Related Commands

Command	Description
iscsi initiator name	Assigns an iSCSI name and changes to iSCSI initiator configuration submode.
islb initiator	Assigns an iSLB name and IP address to the iSLB initiator and enters iSLB initiator configuration submode.
show iscsi initiator	Displays information about configured iSCSI initiators.
show iscsi initiator configured	Displays iSCSI initiator information for the configured iSCSI initiator.
show iscsi initiator detail	Displays detailed iSCSI initiator information.
show iscsi initiator summary	Displays iSCSI initiator summary information.
show islb initiator	Displays iSLB initiator information.
show islb initiator configured	Displays iSLB initiator information for the specified configured initiator.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

stop

To stop SCSI commands in progress on a SAN tuner extension N port, use the **stop** command.

stop {**all** | **command-id** *cmd-id*}

Syntax Description

all	Stops all SCSI commands.
command-id *cmd-id*	Stops a specific SCSI command identified by the command number. The range is 0 to 2147483647.

Command Default

None.

Command Modes

SAN extension N port configuration submode

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example stops all SCSI command on a SAN extension tuner N port:

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# stop all
```

The following example stops a specific SCSI command on a SAN extension tuner N port:

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# stop command-id 100
```

Related Commands

Command	Description
nport pwwn	Configures a SAN extension tuner N port.
read command-id	Configures a SCSI read command for a SAN extension tuner N port.
san-ext-tuner	Enables the SAN extension tuner feature.
show san-ext-tuner	Displays SAN extension tuner information.
write command-id	Configures a SCSI write command for a SAN extension tuner N port.

storage (DMM job configuration submode)

To add a storage port to a DMM job, use the **storage** command in DMM job configuration submode.

storage vsan *vsan-id* **pwwn** *port-wwn* {**existing** | **new**}

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
pwwn *port-wwn*	Specifies the world-wide name of the storage port. The format is hh:hh:hh:hh:hh:hh:hh:hh, where h is a hexadecimal number.
existing	Specifies a port on the existing storage.
new	Specifies a port on the new storage.

Command Default

None.

Command Modes

DMM job configuration submode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add storage information to a DMM job:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# dmm module 3 job 1 create
Started New DMM Job Configuration.
Do not exit sub-mode until configuration is complete and committed
switch(config-dmm-job)# storage vsan 3 pwwn 1d:22:3a:21:3c:44:3b:51 existing
switch(config-dmm-job)#
```

Related Commands

Command	Description
show dmm ip-peer	Displays job information.
show dmm srvr-vt-login	Enables DMM.

streetaddress

To configure the street address with the Call Home function, use the **streetaddress** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

streetaddress *street-address*
no streetaddress *street-address*

Syntax Description

street-address	Specifies the customer's street address where the equipment is located. Allows up to 256 alphanumeric characters in free format for the street number, city, state, and zip (combined).

Command Default

None.

Command Modes

Call Home configuration submode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the street address in the Call Home configuration:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# streetaddress 1234 Picaboo Street, AnyCity, AnyState, 12345
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destinations.
show callhome	Displays configured Call Home information.

subscription

To create a subscription node and enter subscription node configuration mode, use the **subscription** command. To remove the subscription node, use the **no** form of this command.

subscription *id*

no subscription *id*

Syntax Description

id	Sensor subscription ID. Range is from 1 to 4095.

Command Default

No subscription node exists.

Command Modes

Telemetry configuration mode (config-telemetry)

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

Currently, subscription ID supports only numeric ID values.

Examples

This example shows how to create a subscription node and enter subscription node configuration mode:

```
switch# configure
switch(config)# telemetry
switch(config-telemetry)# subscription 100
```

This example shows how to remove the subscription node:

```
switch# configure
switch(config)# telemetry
switch(config-telemetry)# no subscription 100
```

Related Commands

Command	Description
feature telemetry	Enables the SAN Telemetry Streaming feature.
sensor-group	Creates a sensor group and enters sensor group configuration.
show running-config telemetry	Displays the existing telemetry configuration.
show telemetry	Displays telemetry configuration.
telemetry	Enters SAN Telemetry Streaming configuration mode.

suspend

To suspend a switched port analyzer (SPAN) session, use the **suspend** command in SPAN session configuration submode. To disable the suspension, use the **no** form of the command.

suspend
no suspend

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

SPAN session configuration submode

Command History

Release	Modification
6.2(1)	This command was deprecated.
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to suspend a SPAN session:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# span session 1
switch(config-span)# suspend
switch(config-span)# do show span session 1
Session 1 (admin suspended)
   Destination is not configured
   No session filters configured
   Ingress (rx) sources are
     fc3/13,
   Egress (tx) sources are
     fc3/13,
switch(config-span)#
```

The following example shows how to disable the suspension of the SPAN session:

```
switch(config-span)# no suspend
```

Related Commands

Command	Description
destination interface	Configures a SPAN destination interface.
show span session	Displays specific information about a SPAN session.
source	Configures a SPAN source.

Command	Description
span session	Selects or configures the SPAN session and changes to SPAN configuration submode.
switchport	Configures the switch port mode on the Fibre Channel interface.

switchname

To change the name of the switch, use the **switchname** command in configuration mode. To revert the switch name to the default name, use the no form of the command.

switchname *name*
no switchname *name*

Syntax Description

name	Specifies a switch name. Maximum length is 32 characters.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example changes the name of the switch to myswitch1:

```
switch# config terminal
switch(config)# switchname myswitch1
```

The following example changes the name of the switch to the default:

```
myswitch1(config)# no switchname
```

Related Commands

Command	Description
snmp-server	Sets the contact information, switch location, and switch name within the limit of 20 characters (without spaces).

switchport auto-negotiate

To enable autonegotiation on an Ethernet-based SAN extension interface, use the **switchport auto-negotiate** command. To disable autonegotiation, use the **no** form of this command.

switchport auto-negotiate
no switchport auto-negotiate

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.1(1)	This command was introduced.

Usage Guidelines

This command is available only on Ethernet-based SAN extension interfaces, specifically Gigabit Ethernet and IPS type interfaces. It is not available on FCoE Ethernet interfaces or the management interface.

Examples

The following example shows how to enable autonegotiation on a Gigabit Ethernet interface:

```
switch# configure terminal
switch(config)# interface gigabitethernet 2/2
switch(config-if)# switchport auto-negotiate
```

Related Commands

Command	Description
show interface	Displays an interface status and statistics.

switchport beacon

To enable the beacon LED on an interface, use the **switchport beacon** command. To disable the beacon LED on the interface, use the **no** form of this command.

switchport beacon
no switchport beacon

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable the beacon LED on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport beacon
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport description

To specify the description for an interface, use the **switchport description** command. To delete the interface description, use the **no** form of this command.

switchport description *text*
no switchport description *text*

Syntax Description

text	Specifies the interface description. Maximum length is 254 characters.

Command Default

None.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add a description to an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport description Host Linux4943 port 2
```

Related Commands

Command	Description
show interface description	Displays descriptions from all interfaces.

switchport duplex

To specify the Ethernet duplex mode as full, half, or autonegotiate on a management interface, use the **switchport duplex** command. To return the interface to the default mode, use the **no** form of this command.

switchport duplex {**auto** | **full** | **half**}
no switchport duplex {**auto** | **full** | **half**}

Syntax Description

auto	Specifies the duplex mode as autonegotiate.
full	Specifies the duplex mode as full.
half	Specifies the duplex mode as half.

Command Default

The default duplex of the management interface is full.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to set the duplex mode to auto on a management interface:

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# switchport duplex auto
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport encap

To send SPAN traffic through the fabric to a remote switch the SD port must be connected to a neighbor switch and the egress traffic encapsulated in EISL encapsulation to conform to the interswitch frame format. To configure EISL encapsulation on an interface, use the **switchport encap** command. To remove the configuration, use the **no** form of this command.

switchport encap eisl
no switchport encap eisl

Syntax Description

eisl	Specifies extended ISL (EISL) encapsulation on an interface.

Command Default

Disabled.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

This command sets the egress frame format of an interface in the SD port mode. When enabled, all egress frames are encapsulated in the EISL frame format.

Examples

The following example shows how to configure EISL encapsulation on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport encap eisl
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.
show span session	Displays the status of SPAN sessions.

switchport fcbbscn

Credit recovery on Fibre Channel links is facilitated by the buffer to buffer state change notification feature. This allows loss of credits on a link to be detected and recovered. To enable buffer to buffer state change notification on an interface, use the **switchport fcbbscn** command. To disable notification, use the **no** form of this command.

switchport fcbbscn value *value*
no switchport fcbbscn

Syntax Description

value *value*	Specifies the buffer-to-buffer state change number (BB_SC_N). The range is 1 to 15.

Command Default

The default value for **switchport fcbbscn** is enabled for E ports in all releases. Starting with Cisco MDS NX-OS 8.2(1), it is enabled by default for F ports. Starting with Cisco MDS NX-OS 8.4(1), it is enabled by default for NP ports.

The default BB_SC_N value for all port types is 14. A BB_SC_N value of 14 results in buffer to buffer credit recovery primitives being sent in a interval of 16,384 frames/credits.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
8.4(2)	The **value** keyword and *value* variable were introduced.
3.0(1)	This command was introduced.

Usage Guidelines

The BB_SC_N value is the value negotiated between the two sides of the link in the Exchange Link Parameters (ELP) for E ports and in the FLOGI and ACC (FLOGI) for F or NP ports. This value determines the interval for which buffer to buffer recovery primitives are sent and is the exponent of the base of 2. The value negotiated is the larger of the values of the two sides.



Caution This command causes traffic disruption on the specified interface.

Examples

The following example shows how to enable buffer to buffer credit recovery on an interface and set the BB_SC_N to the default value of 14:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport fcbbscn
```

Examples

The following example shows how to specify the BB_SC_N to 7:



Note A BB_SC_N value of 7 results in buffer to buffer credit recovery primitives being sent in a interval of 128 frames/credits.

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport fcbbscn value 7
```

Examples

The following example shows how to disable buffer to buffer credit recovery on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# no switchport fcbbscn
```

Related Commands

Command	Description
show interface counters detailed	Displays the interface counters.

switchport fcrxbbcredit

Each Fibre Channel interface may be assigned receive buffer to buffer credits from 3 types of buffer pools. To configure receive buffer to buffer credits on an interface, use the **switchport fcrxbbcredit** command. To remove the configuration, use the **no** form of this command.

switchport fcrxbbcredit {*std_bufs* [**mode** {**E** | **Fx**}] | **default** | **performance-buffers** {**default***perf_bufs*} | **extended** *ext_bufs*}
no switchport fcrxbbcredit {*std_bufs* [**mode** {**E** | **Fx**}] | **default** | **performance-buffers** {**default** *perf_bufs*} | **extended** *ext_bufs*}

Syntax Description

std_bufs	Specifies count of standard B2B credits. The range is 1 to 500.
mode	(Optional) Restricts the standard receive B2B credit to the specified port mode.
E	Specifies Inter-Switch Link port mode.
Fx	Specifies fixed F and F-loop port modes.
performance-buffers	Configures receive performance buffer allocation on the port.
default	Specifies to use the default credits depending on the port type and capabilities.
perf_bufs	Specifies performance receive B2B credits. The range is 1 to 145.
extended	Configures extended B2B credits.
ext_bufs	Specifies count of extended receive B2B credits. The range is 256 to 4095.

Command Default

None.

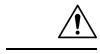
Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 2.0(1b)	Added the **extended** keyword to the syntax.
NX-OS 1.1(1)	This command was introduced.

Usage Guidelines



Caution This command causes traffic disruption on the specified interface.

Configure the **feature fcrxbbcredit extended** command to enable access to the **switchport fcrxbbcredit** command. The **switchport fcrxbbcredit** command will not be available until the extended credit feature is enabled.

Extended buffer to buffer credits are intended for long haul links where a high RTT causes more frames to be in flight than normal at linerate. They are advertised to the link peer and require an ENTERPRISE_PKG license.

Performance buffers are intended to absorb short bursts on higher speed ingress interfaces destined for lower speed or mildly congested egress interfaces. They are internal to the switch and are not advertised to the link peer. They are only available in 12-port 4-Gbps and 4-port 10 Gbps switching modules.

Examples

The following example shows how to configure default credits on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport fcrxbbcredit default
```

Related Commands

Command	Description
feature fcrxbbcredit extended	Enables extended receive B2B credits.
show interface	Displays interface status and statistics.

switchport fcrxbufsize

To configure the maximum size of the receive data buffer on an interface, use the **switchport fcrxbufsize** command. To remove the configuration, use the **no** form of this command.

switchport fcrxbufsize *buffer-size*
no switchport fcrxbufsize *buffer-size*

Syntax Description

buffer-size	Specifies maximum frame size for the interface. The range is 256 to 2112 bytes.

Command Default

The default receive data buffer size is 2112 bytes.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines



Caution This command causes traffic disruption on the specified interface.

Examples

The following example shows how to set the frame size for an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport fcrxbufsize 256
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport fec

To configure the Forward Error Correction (FEC) on an interface, use the **switchport fec** command. To remove the configuration, use the **no** form of this command.

switchport fec
no switchport fec

Syntax Description

fec	Configures the FEC state on an interface.

Command Default

Disabled.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
9.2(1)	Both Forward Error Correction (FEC) and Transmitter Training Signal (TTS) must be configured on Cisco MDS 48-Port 64-Gbps Fibre Channel Switching Module (DS-X9748-3072K9) to use FEC at 16-Gbps speed. A warning message is displayed in the **switchport fec** command output when only FEC is configured.
6.2(7)	This command was introduced.

Usage Guidelines

Caution This command causes traffic disruption on the specified interface.

Note This command is only accepted on ports with the speed fixed to 16 Gbps and FEC already enabled.

Use the **switchport fec** command in the interface configuration mode to configure FEC on an interface.

Note FEC TTS is supported on the DS-X9448-768K9 Generation 5 module in Cisco MDS NX-OS Release 6.2(11c) and later 6.2(11x) releases, and Cisco MDS NX-OS Release 6.2(15) and later releases. It is not supported in Cisco MDS NX-OS Release 6.2(13).

Examples

The following example shows how to configure FEC on a Fibre Channel interface:

```
switch# config t
switch(config)# interface fc 1/1
switch(config-if)# switchport fec
```

The following example shows a warning message that TTS must be configured on the Cisco MDS 48-Port 64-Gbps Fibre Channel Switching Module (DS-X9748-3072K9) to use FEC at 16-Gbps speed:

```
switch# config t
switch(config)# interface fc7/1
switch(config-if)# switchport speed 16000
switch(config-if)# switchport fec
fc7/1: (warning) FEC on this module requires TTS to function at 16 Gbps. Please configure
'switchport fec tts'.
```

To resolve this error, configure the **switchport fec tts** command on the interface.

Related Commands

Command	Description
show interface fc	Displays the status of the specified Fibre Channel interface.

switchport fec tts

To configure the Forward Error Correction (FEC) and the Transmitter Training Signal (TTS) on an interface, use the **switchport fec tts** command. To remove the configuration, use the **no** form of this command.

switchport fec [**tts**]
no switchport fec [**tts**]

Syntax Description

tts	(Optional) Enables Transmitter Training Signal (TTS) allowing negotiation of FEC capability.

Command Default

Disabled.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 6.2(11c)	This command was introduced.

Usage Guidelines

Caution This command causes traffic disruption on the specified interface.

Note This command is only accepted on ports with the speed fixed to 16 Gbps and FEC already enabled.

Use the **switchport fec tts** command only after configuring FEC using the **switchport fec** command.

The TTS is not used by 4 and 8-Gbps Fibre Channel ports. From 32 Gbps and higher, its use is mandatory. For 16 Gbps Fibre Channel ports, EA variants must transmit the TTS during the link speed negotiation, but the use of it by the receiver is optional, and EL variants must not use TTS.

Note FEC TTS is supported on the DS-X9448-768K9 Generation 5 module in Cisco MDS NX-OS Release 6.2(11c) and later 6.2(11x) releases and Cisco MDS NX-OS Release 6.2(15) and later releases. It is not supported in Cisco MDS NX-OS Release 6.2(13).

Examples

The following example show how to configure FEC with TTS on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport fec
switch(config-if)# switchport fec tts
```

Related Commands

Command	Description
show interface fc	Displays the status of the specified Fibre Channel interface.

switchport fill-pattern

To configure the link fill pattern on an interface, use the **switchport fill-pattern** command.

switchport fill-pattern {**IDLE** | **ARBFF**} **speed 8000**

Syntax Description

IDLE	Configures the fill pattern as IDLE.
ARBFF	Configures the fill pattern as ARBff.
speed	Select speed to apply setting to.
8000	Specifies 8-Gbps link speed.

Command Default

The default setting for the link fill pattern is ARBff.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 5.2(6)	This command was introduced.

Usage Guidelines

Caution This command causes traffic disruption on the specified interface.

Examples

The following example shows how to configure the fill pattern as ARBff on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport fill-pattern ARBFF speed 8000
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport ignore

To prevent the detection of certain error events from disabling Fibre Channel interfaces, use the **switchport ignore** command. To revert to the default settings, use the **no** form of this command.

switchport ignore {**bit-errors** | **interrupt-thresholds**}
no switchport ignore {**bit-errors** | **interrupt-thresholds**}

Syntax Description

bit-errors	Ignore the bit errors.
interrupt-thresholds	Ignore interrupt thresholds.

Command Default

None.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 6.2	The **interrupt-thresholds** keyword was added.
NX-OS 2.1(1a)	This command was introduced.

Usage Guidelines

The bit error rate threshold is used by the switch to detect an increased error rate before performance degradation seriously affects traffic.

Bit errors can occur for the following reasons:

- Faulty or bad cable
- Faulty or bad GBIC or SFP
- GBIC or SFP is specified to operate at 1 Gbps, but is used at 2 Gbps
- Short haul cable is used for long haul or long haul cable is used for short haul
- Momentary sync loss
- Loose cable connection at one or both ends
- Improper GBIC or SFP connection at one or both ends

A bit error rate threshold is detected when 15 error bursts occur in a 5-minute period. By default, the switch disables the interface when the threshold is reached. After fixing the source of the bit errors, an affected interface should be re-enabled with the **shutdown** and **no shutdown** command sequence.

Interrupts thresholds are used by the switch to detect excessive internal interrupts before they affect switch performance.

Interrupt thresholds can occur because of continuous primitive sequence (NOS/OLS/LR/LRR).



Note Regardless of the setting of the **switchport ignore bit-errors** command, the switch generates a syslog message when bit error threshold events are detected.

Examples

The following example shows how to prevent the detection of bit error events from disabling an interface:

```
switch# configure terminal
switch(config)# interface fc1/1
switch(config-if)# switchport ignore bit-errors
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport ingress-rate

To configure the port rate limit for a specified interface, use the **switchport ingress-rate** command in interface configuration mode. Use the **no** form of the command to delete the configured switch port information.

switchport ingress-rate *limit*
no switchport ingress-rate *limit*

Syntax Description

limit	Specifies the ingress rate limit as a percentage. The range is 1 to 100.

Command Default

Disabled.

Command Modes

Interface configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Access this command from the switch(config-if)# submode. This command is only available if the following conditions are true:

- The QoS feature is enabled using the **qos enable** command.
- The command is entered in a Cisco MDS 9100 series switch.

Examples

The following example configures the ingress rate limit on a Fibre Channel interface:

```
switch# config terminal
switch(config)# interface fc 2/5
switch(config-if)# switchport ingress-rate 5
```

Related Commands

Command	Description
show interface fc	Displays an interface configuration for a specified Fibre Channel interface.

switchport initiator id

To configure the iSCSI initiator ID mode, use the **switchport initiator id** command in interface configuration submode. To delete the iSCSI initiator ID mode, use the **no** form of the command.

switchport initiator id {*ip-addressname*}
no switchport initiator id {*ip-addressname*}

Syntax Description

ip-address	Identifies initiators using the IP address.
name	Identifies initiators using the specified name.

Command Default

The iSCSI initiator ID mode is disabled.

Command Modes

Interface configuration submode under the **iscsi interface x/x** command

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the iSCSI initiator ID mode for an iSCSI interface:

```
switch# config terminal
switch(config)# interface iscsi 2/5
switch(config-if)# switchport initiator id ip-address
switch(config-if)# switchport initiator name
```

Related Commands

Command	Description
show interface iscsi	Displays an interface configuration for a specified iSCSI interface.

switchport link-diag

To enable the link diagnostic mode on a diagnostic port, use the **switchport link-diag** command in interface configuration mode. To exit the link diagnostic mode, use the **no** form of this command.

switchport link-diag

no switchport link-diag

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration mode (config-if)

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

The diagnostic port must be in admin shutdown status to enter the link diagnostic mode.

The following example shows how to configure the link diagnostic mode on a diagnostic port:

```
configure terminal
 interface fc 1/1
  shutdown
  switchport link-diag
  no shutdown
  end
```

The following example shows how to unconfigure the link diagnostic mode on a diagnostic port:

```
configure terminal
 interface fc 1/1
  shutdown
  no switchport link-diag
  no shutdown
  end
```

Related Commands

Command	Description
diagnostic result interface fc test link-diag	Displays the results of the link diagnostics tests that are performed on a diagnostic port.
diagnostic start interface fc test link-diag	Runs link diagnostics tests on a diagnostic port.
diagnostic stop interface fc test link-diag	Stops the link diagnostics tests that are running on a diagnostic port.

Command	Description
show diagnostic test link-diag status	Checks the status of the link diagnostics tests that are running on the switch.

switchport max-npiv-limit

To configure the maximum number of logins that are allowed on a nontrunking interface, use the **switchport max-npiv-limit** command. To remove the configuration, use the **no** form of this command.

switchport max-npiv-limit *max-npivs*
no switchport max-npiv-limit *max-npivs*

Syntax Description

max-npivs	Specifies the maximum logins for the interface. The range is from 1 to 256.

Command Default

None.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 6.2(7)	This command was introduced.

Usage Guidelines

Note Both **switchport max-npiv-limit** and **switchport trunk-max-npiv-limit** commands can be configured on a port or Port Channel. The current port mode determines the type of configuration used. If the port is nontrunking, the **max-npiv-limit** setting is used. If the port is trunking, the **trunk-max-npiv-limit** setting is used.

If a login limit is reached on a port and it receives a login request, then a syslog message is logged and the login rejected.

Examples

The following example shows how to configure the maximum number of logins on an F-port to 4:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport max-npiv-limit 4
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.
switchport trunk-max-npiv-limit	Configures the maximum number of logins that are allowed on a trunk port.

switchport mode

To configure the Fibre Channel mode of an interface, use the **switchport mode** command. To remove the configuration, use the **no** form of this command.

switchport mode {**E** | **F** | **FL** | **Fx** | **NP** | **SD** | **ST** | **auto**}
no switchport mode {**E** | **F** | **FL** | **Fx** | **NP** | **SD** | **ST** | **auto**}

Syntax Description

E	Configures fixed Inter-Switch Link port mode.
F	Specifies fixed F port mode.
FL	Specifies fixed F-loop port mode.
Fx	Specifies fixed F and F-loop port modes.
NP	Specifies fixed N port virtualizer mode.
SD	Specifies fixed SPAN destination port mode.
ST	Specifies fixed trunked SPAN port mode.
auto	Specifies autosense mode.

Command Default

The default port mode is auto.

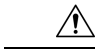
Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 4.1(3)	Added the **F** and **NP** port mode.
NX-OS 3.0(1)	Added the **ST** option to the syntax.
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines



Caution This command causes traffic disruption on the specified interface.

A port must be in dedicated mode before it can be set to **E** mode.

Examples

The following example shows how to configure fixed Inter-Switch Link mode on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport mode E
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.
show port-resources	Displays the rate mode of module ports.

switchport mtu

To configure the Ethernet layer maximum transmission unit (MTU) on an Ethernet-based SAN extension interface, use the **switchport mtu** command. To remove the configuration, use the **no** form of this command.

switchport mtu *size*
no switchport mtu *size*

Syntax Description

size	Specifies the MTU size in bytes. The range is 576 to 9216.

Command Default

The default size is 1500 bytes.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

This command is available only on Ethernet-based SAN extension interfaces, specifically Gigabit Ethernet and IPS type interfaces. It is not available on FCoE Ethernet interfaces or the management interface.

Examples

The following example shows how to configure the Ethernet MTU to 3000 bytes on a Gigabit Ethernet interface:

```
switch# configure terminal
switch(config)# interface gigabitethernet 2/2
switch(config-if)# switchport mtu 3000
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport link-negotiation early-tc

MDS 64 Gbps capable FC interfaces enforce strict compliance to the Fibre Channel link initialization standards. This includes a requirement at 32 Gbps speed that Link Speed Negotiation (LSN) be completed before the Training Complete (TC) indication is sent. However, some devices incorrectly require TC indication to be set simultaneously with LSN complete during link negotiation. Use the **switchport link-negotiation early-tc** command to enable sending training complete simultaneously with link speed negotiation complete on 64 Gbps FC switch ports at 32 Gbps speed. If you configure this option and the link speed negotiates to a speed other than 32 Gbps, the system ignores this option.

Use the **no** option to disable this behaviour and used standards compiant link negotiation.

[no] switchport link-negotiation early-tc

Command Default

Disabled.

Command Modes

Interface configuration submode

Command History

Release	Modification
9.4(5)	This command was introduced.

Usage Guidelines

This command controls the link negotiation link training behavior at 32 Gbps link speed and mode F. Ensure that the interface is configured to mode F before changing this setting.

This command must be disabled on all interfaces where it was enabled before an In-Service Software Downgrade (ISSD) to a lower software version that does not support this feature. Failure to do so will prevent the downgrade.

Examples

Thefollowing example shows how to enable non standards-compliant link training behavior at 32 Gbps speed:

```
switch# configure terminal
switch(config)# interface fc1/1
switch(config-if)# switchport mode f
switch(config-if)# switchport link-negotiation early-tc
```

The following example shows how to display the link training behavior at 32 Gbps speed:

```
switch# show interface fc1/1 | include negotiation
Link negotiation early TC is on
```

Related Commands

Command	Description
switchport mode	Configures the Fibre Channel mode of an interface.
switchport speed	Configures the speed of an interface.
show interface	Displays the status of an interface.

switchport owner

To configure a descriptive owner string on an interface, use the **switchport owner** command. To remove the configuration, use the **no** form of this command.

switchport owner *owner*
no switchport owner

Syntax Description

owner	(Optional) Specifies the owner. The maximum length of the string is 80 characters.

Command Default

None.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the owner string on an interface:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch (config)# interface fc1/1
Switch (config-if)# switchport owner StorageOps
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport promiscuous-mode

To enable promiscuous mode on an Ethernet-based SAN extension interface, use the **switchport promiscuous-mode** command. To disable the promiscuous mode, use the **no** form of this command.

switchport promiscuous-mode {**off** | **on**}
no switchport promiscuous-mode {**off** | **on**}

Syntax Description

off	Disables promiscuous mode on an interface.
on	Enables promiscuous mode on an interface.

Command Default

Disabled.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.1(1)	This command was introduced.

Usage Guidelines

This command is available only on Ethernet-based SAN extension interfaces, specifically Gigabit Ethernet and IPS type interfaces. It is not available on FCoE Ethernet interfaces or the management interface.

Examples

The following example enables promiscuous mode on a Gigabit Ethernet interface:

```
switch# configure terminal
switch(config)# interface gigabitethernet 2/2
switch(config-if)# switchport promiscuous-mode on
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport proxy-initiator

To configure the iSCSI proxy initiator mode on an iSCSI interface, use the **switchport proxy-initiator** command in interface configuration submode. To delete the iSCSI proxy initiator mode, use the **no** form of the command.

switchport proxy-initiator [**nwwn** *wwn* **pwwn** *wwn*]
no switchport proxy-initiator [**nwwn** *wwn* **pwwn** *wwn*]

Syntax Description

nwwn *wwn*	(Optional) Specifies the node WWN.
pwwn *wwn*	(Optional) Specifies the port WWN.

Command Default

The iSCSI proxy initiator mode is disabled.

Command Modes

Interface configuration submode under the **iscsi interface x/x** command

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

When you do not include the WWNs in the command, the IPS port dynamically assigns a pWWN and nWWN to the proxy initiator.

Caution Enabling proxy initiator mode on an iSCSI interface that is part of an iSLB VRRP group impacts load balancing on the interface.

Examples

The following example configures the iSCSI proxy initiator mode for a iSCSI interface using WWNs:

```
switch# config terminal
switch(config)# interface iscsi 2/5
switch(config-if)# switchport proxy-initiator nwwn 11:11:11:11:11:11:11:11 pwwn
22:22:22:22:22:22:22:22
```

The following example configures the iSCSI proxy initiator mode for a iSCSI interface without WWNs:

```
switch# config terminal
switch(config)# interface iscsi 2/5
switch(config-if)# switchport proxy-initiator
```

The following example deletes the iSCSI proxy initiator mode for a iSCSI interface:

```
switch(config-if)# switchport proxy-initiator
```

Related Commands

Command	Description
show interface iscsi	Displays an interface configuration for a specified iSCSI interface.

switch-priority

To configure the switch priority with the Call Home function, use the **switch-priority** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

switch-priority *priority-value*

Syntax Description

priority-value	Specifies the priority level. 0 is the highest priority and 7 the lowest.

Command Default

- You cannot disable this command. You can only set to default.

  7 is the default value.

Command Modes

Call Home configuration submode

Command History

Release	Modification
4.1(1b)	Added usage guidelines.
1.0(2)	This command was introduced.

Usage Guidelines

The Call Home switch priority is specific to each switch in the fabric. It is set by the switch administrator to guide the operations personnel who receive the Call Home messages as to which messages should be serviced first. For example, the switch priority of a trading floor switch may be set higher than that of a switch in a tape backup network because the trading floor users may not be able to tolerate as much service interruption as the backup network.

Examples

The following example shows how to configure the switch priority in the Call Home configuration:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# switch-priority 0
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

switchport rate-mode

Each interface belongs to a *port group* and each port group has access to a preallocated subset of the backplane bandwidth. On full bandwidth modules, all interfaces have access to the backplane bandwidth at maximum interface speed. On oversubscribed modules, the total of the maximum interface speeds exceeds the allocated backplane bandwidth of the port group. To configure the port group bandwidth-allocation mode of an interface, use the **switchport rate-mode** command. To remove the configuration, use the **no** form of this command.

switchport rate-mode {**dedicated** | **shared**}
no switchport rate-mode {**dedicated** | **shared**}

Syntax Description

dedicated	Specifies dedicated bandwidth for the interface.
shared	Specifies shared bandwidth for the interface.

Command Default

For oversubscribed modules, the default port group mode is shared. For full bandwidth modules, the only available mode is dedicated.

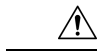
Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 3.0(1)	This command was introduced.

Usage Guidelines



Caution This command causes traffic disruption on the specified interface.

The maximum port speed of an interface, combined with the rate mode, determines the amount of shared resources available to the ports in the port group. In the case of dedicated rate mode, the port group resources are reserved even though the bandwidth is not used. For oversubscribed port groups, if an interface is configured for autosensing (**auto**) then bandwidth equal to the maximum supported speed of the interface is reserved, even if the link comes up at a lower speed. If the autosensing maximum speed is configured (for example, **auto max 8000**) then only that much bandwidth is reserved and the remaining possible bandwidth is available for other interfaces in the port group.

Table 1: Default Speed and Buffer Configuration

Switching Module	Speed	Port Mode	Rate Mode	Receive Credits (min/max/default)
DS-X9304-18K9, Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4)	1, 2, or 4 Gbps	Fx	Shared	1/16/16
		Fx	Dedicated	2/250/16
		E-port	Dedicated	2//250/250

Switching Module	Speed	Port Mode	Rate Mode	Receive Credits (min/max/default)
DS-C9222i-K9, Cisco MDS 9222i Switch	1, 2, or 4 Gbps	Fx	Shared	1/16/16
		Fx	Dedicated	2/250/16
		E-port	Dedicated	2//250/250
DS-X9704, Cisco MDS 9000 Family 4-Port 10-Gbps Fibre Channel Switching Module	10 Gbps	NA	Shared	NA
		Fx	Dedicated	2/750/16
		E-port	Dedicated	2/750/750
DS-X9248-48K9, Cisco MDS 9000 4/44-Port Host-Optimized 8-Gbps Fibre Channel Switching Module	1, 2, 4, or 8 Gbps	Fx	Shared	1/32/32
		Fx	Dedicated	2/250/32
		E-port	Dedicated	2/250/125
DS-X9248-96K9, Cisco MDS 9000 48-Port 8-Gbps Fibre Channel Switching Module	1, 2, 4, or 8 Gbps	Fx	Shared	1/32/32
		Fx	Dedicated	2/500/32
		E-port	Dedicated	2/500/250
DS-X9224-96K9, Cisco MDS 9000 24-Port 8-Gbps Fibre Channel Switching Module	1, 2, 4, or 8 Gbps	Fx	Shared	1/32/32
		Fx	Dedicated	2/500/32
		E-port	Dedicated	2/500/500
DS-C9148-K9, Cisco MDS 9148 48-Port Multilayer Fabric Switch	1, 2, 4, or 8 Gbps	NA	Shared	NA
		Fx	Dedicated	1/125/32
		E-port	Dedicated	1/125/32
DS-C9134-K9, Cisco MDS 9134 34-Port Multilayer Fabric Switch	1, 2, or 4 Gbps	NA	Shared	NA
		Fx	Dedicated	1/61/16
		E-port	Dedicated	1/61/16
DS-C9124-K9, Cisco MDS 9124 24-Port Multilayer Fabric Switch	1, 2, or 4 Gbps	NA	Shared	NA
		Fx	Dedicated	1/61/16
		E-port	Dedicated	1/61/16
DS-C9134-K9, Cisco MDS 9134 32-Port Fabric Switch	1, 2, or 4 Gbps	NA	Shared	NA
		Fx	Dedicated	1/61/64
		E-port	Dedicated	2/61/64

Switching Module	Speed	Port Mode	Rate Mode	Receive Credits (min/max/default)
DS-C9124, Cisco MDS 9124 24-Port Fabric Switch	1, 2, or 4 Gbps	Fx	Shared	2/16/16
		Fx	Dedicated	2/250/16
		E-port	Dedicated	2/250/250
DS-C9222i-K9, Cisco MDS 9222i 18-Port Multiservice Modular Switch	1, 2, or 4 Gbps	Fx	Shared	2/16/16
		Fx	Dedicated	2/250/16
		E-port	Dedicated	2/250/250
DS-X9248-256K9, Cisco MDS 9000 48-Port Advanced Fibre Channel Module	1, 2, 4, or 8 Gbps	Fx	Shared	1/125/32
		Fx	Dedicated	2/250/16
DS-X9232-256K9, Cisco MDS 9000 32-Port Advanced Fibre Channel Module	1, 2, 4, or 8 Gbps	Fx	Shared	1/125/32
		Fx	Dedicated	2/250/16

When configuring port modes, observe the following guidelines:

- Auto port mode and E port mode cannot be configured in the shared rate mode.
- The 4-port 10-Gbps module does not support the FL port mode.
- Generation 2 modules do not support the TL port mode.
- Shared to dedicated ports must be configured in the following order: speed, rate mode, port mode, and credit.
- Dedicated to shared ports must be configured in the following order: credit, port mode, rate mode, and speed.

When configuring port channels, observe the following guidelines:

- When an interface is out of service, it cannot be part of a port channel.
- The 24-port module and the 48-port module support making ports out of service. In a shared resource configuration, an out-of-service port reverts to its default values when it comes back into service.
- The maximum number of port channels for Generation 2 modules is 256.
- The number of port channels is independent of the type of supervisor module.
- When using the **force** option to add a port channel to a configuration that uses Generation 2 modules, the force addition can fail for a Generation 2 interface if resources are unavailable.

Examples

The following example reserves shared (default) bandwidth for an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport rate-mode shared
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.
show port-resources	Displays the rate mode of module ports.

switchport speed

To configure the speed of an interface, use the **switchport speed** command. To return to the default speed, use the **no** form of this command.

switchport speed {**1000** | **2000** | **4000** | **8000** | **10000** | **16000** | **auto** [**max** {**2000** | **4000** | **8000** | **16000**}]}
no switchport speed {**1000** | **2000** | **4000** | **8000** | **10000** | **16000** | **auto** [**max** {**2000** | **4000** | **8000** | **16000**}]}

Syntax Description

1000	Configure the link speed to be fixed at 1-Gbps speed.
2000	Configure the link speed to be fixed at 2-Gbps speed.
4000	Configure the link speed to be fixed at 4-Gbps speed.
8000	Configure the link speed to be fixed at 8-Gbps speed.
10000	Configure the link speed to be fixed at 10-Gbps speed.
16000	Configure the link speed to be fixed at 16-Gbps speed.
auto	Configures autosense speed.
max 2000	(Optional) Limits maximum link speed to 2 Gbps.
max 4000	(Optional) Limits maximum link speed to 4 Gbps.
max 8000	(Optional) Limits maximum link speed to 8 Gbps.
max 16000	(Optional) Limits maximum link speed to 16 Gbps.

Command Default

The default speed mode is auto.

The default maximum autosense speed is the maximum port speed.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 3.0(1)	Added the **4000** option to the **speed** keyword.
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the speed of a Fibre Channel interface to be fixed at 16 Gbps:

```
switch# configure terminal
```

```
switch(config)# interface fc 1/1
switch(config-if)# switchport speed 16000
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport trunk allowed vsan

To configure the list of allowed VSANs on a trunk link, use the **switchport trunk allowed vsan** command. To remove the configuration, use the **no** form of this command.

switchport trunk allowed vsan {**add** *vsan-id* | **all** | *vsan-id* [**no-warning**]}

Syntax Description

add	Configure additional allowed VSANs to the existing list.
vsan-id	Specifies the VSAN ID. The range is 1 to 4093.
all	Adds all VSANs to the allowed VSAN list.

Command Default

All VSANs are allowed.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

If the allowed VSANs on a trunk are a set of noncontiguous VSANs, use the **switchport trunk allowed vsan** *vsan-id* command first and then use the **switchport trunk allowed vsan add** command to complete the set of desired VSANs. The commands in the configuration are automatically rebuilt in numerical order by NX-OS.

Examples

The following example shows how to limit the VSANs on an interface to VSAN 10 to 20 and 50:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport trunk allowed vsan 10-20
switch(config-if)# switchport trunk allowed vsan add 50
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport trunk-max-npiv-limit

To configure the maximum number of logins that are allowed on a trunking interface, use the **switchport trunk-max-npiv-limit** command. To remove the configuration, use the **no** form of this command.

switchport trunk-max-npiv-limit *max-npivs*
no switchport trunk-max-npiv-limit *max-npivs*

Syntax Description

max-npivs	Specifies the maximum NPVI logins per trunk interface. The range is from 1 to 512.

Command Default

None.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 6.2(7)	This command was introduced.

Usage Guidelines

Both **switchport max-npiv-limit** and **switchport trunk-max-npiv-limit** commands can be configured on a port or Port Channel. The current port mode determines the type of configuration used. If the port is nontrunking, the **max-npiv-limit** setting is used. If the port is trunking, the **trunk-max-npiv-limit** setting is used.

If a login limit is reached on a port and it receives a login request, then a syslog message is logged and the login rejected.

Examples

The following example shows how to configure the maximum number of allowed logins on a trunking interface to 500:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport trunk-max-npiv-limit 500
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.
switchport max-npiv-limit	Configures the maximum number of logins that are allowed on a port.

switchport trunk mode

To specify the trunk mode for an interface, use the **switchport trunk mode** command. To remove the configuration, use the **no** form of this command.

switchport trunk mode {**auto** | **off** | **on**}
no switchport trunk mode {**auto** | **off** | **on**}

Syntax Description

auto	Specifies the trunk mode to be auto.
off	Disables trunking mode.
on	Enables trunking mode.

Command Default

The default trunk mode is **on**.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

Caution This command causes traffic disruption on the specified interface.

Note During ISSU, the admin trunk mode is set to **off** for up and operationally non trunking ports to avoid network disruption due to misbehaving peer devices.

By default, trunk mode is enabled on all Fibre Channel interfaces (modes E, F, FL, Fx, ST, and SD) on non-NPV switches. On NPV switches, by default, trunk mode is disabled. You can configure trunk mode as on (enabled), off (disabled), or auto (automatic). The trunk mode configuration at the two ends of an ISL, between two switches, determine the trunking state of the link and the port modes at both ends.

Table 2: Trunk Mode Status Between Switches

Configured Trunk Mode			Resulting State and Port Mode	
Port Type	**Switch 1**	**Switch 2**	**Trunking State**	**Port Mode**
E ports	On	Auto or on	Trunking (EISL)	TE port
	Off	Auto, on, or off	No trunking (ISL)	E port
	Auto	Auto	No trunking (ISL)	E port

Configured Trunk Mode			Resulting State and Port Mode	
Port Type	**Switch 1**	**Switch 2**	**Trunking State**	**Port Mode**
Port Type	**Core Switch**	**NPV Switch**	**Trunking State**	**Link Mode**
F and NP ports	On	Auto or on	Trunking	TF-TNP link
	Auto	On	Trunking	TF-TNP link
	Off	Auto, on, or off	No trunking	F-NP link

Examples

The following example shows how to set the trunk mode to auto on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport trunk mode auto
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switch-wwn

To configure a switch WWN in an autonomous fabric ID (AFID) database, use the **switch-wwn** command in AFID database configuration submode. To disable this feature, use the **no** form of this command.

switch-wwn *wwn-id* {**autonomous-fabric-id** *fabric-id* **vsan-ranges** *vsan-range* | **default-autonomous-fabric-id** *fabric-id* **vsan-ranges** *vsan-range*}
no switch-wwn *wwn-id* {**autonomous-fabric-id** *fabric-id* **vsan-ranges** *vsan-range* | **default-autonomous-fabric-id** *fabric-id***vsan-ranges** *vsan-range*}

Syntax Description

wwn-id	Specifies the port WWN, with the format hh:hh:hh:hh:hh:hh:hh:hh.
autonomous-fabric-id *fabric-id*	Specifies the fabric ID for the IVR topology.
vsan-ranges *vsan-range*	Specifies the IVR VSANs or range of VSANs. The range of values for a VSAN ID is 1 to 4093.
default-autonomous-fabric-id *fabric-id*	Specifies the default fabric ID for the IVR topology.

Command Default

Disabled.

Command Modes

AFID database configuration submode

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

Using the default-autonomous-fabric-id keyword configures the default AFID for all VSANs not explicitly associated with an AFID.

Examples

The following example adds a switch WWN, an AFID, and a range of VSANs to the AFID database:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ivr vsan-topology ?
  activate  Activate VSAN topology database for inter-VSAN routing
  auto      Enable discovery of VSAN topology for inter-VSAN routing
  database  Configure VSAN topology database for inter-VSAN routing
switch(config)# ivr vsan-topology auto
switch(config)# autonomous-fabric-id database
AFID database is used only when VSAN Topology is in AUTO mode
switch(config-afid-db)# ?
autonomous-fabric-id cfg. cmd:
  do          EXEC command
  exit        Exit from this submode
  no          Negate a command or set its defaults
  switch-wwn  Enter Switch WWN of a switch
switch(config-afid-db)# switch ?
  <hh:hh:hh:hh:hh:hh:hh:hh>  Enter a WWN in dotted hex notation
```

```
switch(config-afid-db)# switch 28:1d:00:05:30:00:06:ea ?
  autonomous-fabric-id          Enter Autonomous Fabric ID
  default-autonomous-fabric-id  Enter default Autonomous Fabric ID
switch(config-afid-db)# switch 28:1d:00:05:30:00:06:ea autonomous-fabric-id ?
  <1-64>  Enter an autonomous fabic ID
switch(config-afid-db)# switch 28:1d:00:05:30:00:06:ea autonomous-fabric-id 14 ?
  vsan-ranges  Enter VSANs in this autonomous-fabric-id at this switch
switch(config-afid-db)# switch 28:1d:00:05:30:00:06:ea autonomous-fabric-id 14 v
san-ranges ?
  <1-4093>  Enter upto 5 ranges of VSAN identifiers
switch(config-afid-db)# switch 28:1d:00:05:30:00:06:ea autonomous-fabric-id 14 vsan-ranges
 1-4 ?
  ,     Comma
  <cr>  Carriage Return
switch(config-afid-db)# switch-wwn 28:1d:00:05:30:00:06:ea autonomous-fabric-id 14 vsan-ranges
 1-4
```

The following example adds a switch WWN and the default AFID to the AFID database:

```
switch(config-afid-db)# ?
autonomous-fabric-id cfg. cmd:
  do          EXEC command
  exit        Exit from this submode
  no          Negate a command or set its defaults
  switch-wwn  Enter Switch WWN of a switch
switch(config-afid-db)# switch-wwn ?
  <hh:hh:hh:hh:hh:hh:hh:hh>  Enter a WWN in dotted hex notation
switch(config-afid-db)# switch-wwn 28:1d:00:05:30:00:06:ea ?
  autonomous-fabric-id          Enter Autonomous Fabric ID
  default-autonomous-fabric-id  Enter default Autonomous Fabric ID
switch(config-afid-db)# switch-wwn 28:1d:00:05:30:00:06:ea default-autonomous-fabric-id ?
  <1-64>  Enter a default autonomous fabic ID
switch(config-afid-db)# switch-wwn 28:1d:00:05:30:00:06:ea default-autonomous-fabric-id 16
 ?
  <cr>  Carriage Returnswitch(config-afid-db)# switch-wwn 28:1d:00:05:30:00:06:ea
default-autonomous-fabric-id 16
```

Related Commands

Command	Description
autonomous-fabric-id-database	Enters AFID database configuration submode.
show autonomous-fabric-id-database	Displays the contents of the AFID database.

system cores

To enable copying the core and log files periodically, use the **system cores** command in configuration mode. To revert the switch to factory defaults, use the **no** form of the command.

system cores {**slot0:** | **tftp:**}
no system cores

Syntax Description

slot0:	Selects the destination file system.
tftp:	Selects the destination file system.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Create any required directory before entering this command. If the directory specified by this command does not exist, the switch software logs a syslog message each time a copy cores is attempted.

Examples

The following example enables periodic copying core and log files:

```
switch# config terminal
switch(config)# system cores slot0:coreSample
```

The following example disables periodic copying core and log files:

```
switch(config)# no
 system cores
```

Related Commands

Command	Description
show system cores	Displays the currently configured scheme for copying cores.

system counter

fc-abort sequence frames (FC ABTS) can be sent by both initiators and targets when an FC exchange times out. To include the transmitted fc-aborts counter in the output of the **show interface** commands, use the **system counter fc-aborts**command. The fc-aborts counter counts the number of FC ABTS frames transmitted by the interface. Use the **no** form to disable the command.

[no]system counter fc-aborts

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
9.4(5)	This command was introduced.

Usage Guidelines

fc-abort sequence counter is supported starting from Cisco MDS NX-OS 9.4(5) on the following modules and switches:

- Cisco MDS 9700 48-port 64-Gbps Switching Module (DS-X9748-3072K9)
- Cisco MDS 9700 48-Port 32-Gbps Fibre Channel Switching Module (DS-X9648-1536K9)
- Cisco MDS 9396V 64-Gbps 96-Port Fibre Channel switch
- Cisco MDS 9148V 64-Gbps 48-Port Fibre Channel switch
- Cisco MDS 9124V 64-Gbps 24-Port Fibre Channel Switch
- Cisco MDS 9148T 32-Gbps 48-Port Fibre Channel Switch
- Cisco MDS 9396T 32-Gbps 96-Port Fibre Channel Switch
- Cisco MDS 9132T 32-Gbps 32-Port Fibre Channel Switch

Examples

The following example enables counting of transmitted FC abort sequence frames:

```
switch# config terminal
switch(config)# system counter fc-aborts
```

The following example disables counting of transmitted FC abort sequence frames:

```
switch # configure terminal
switch(config)# no system counter fc-aborts
```

The following example verifies if the **system counter fc-aborts** command is enabled:

```
switch# show running-config all | grep aborts
system counter fc-aborts
```

Related Commands

Command	Description
clear counters	Clear interface counters.
show interface counters	Display interface counters.
show interface	Displays the status of an interface.
show interface counters detailed	Displays the interface counters.

system default interface congestion mode

To configure the default interface congestion mode, use the **system default interface congestionmode** command. To disable this feature, use the **no** form of the command.

system default interface congestion mode {**core** | **edge**}
no system default interface congestion mode {**core** | **edge**}

Syntax Description

core	Specifies the core port type.
edge	Specifies the edge port type.

Command Default

None.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure the default interface congestion mode for the core port type:

```
switch# config terminal
switch(config)# system default interface congestion mode core
switch(config)#
```

The following example shows how to disable the default interface congestion mode for the edge port type:

```
switch# config terminal
switch(config)# no system default interface congestion mode edge
switch(config)#
```

Related Commands

Command	Description
show interface brief	Displays FC port modes.
show system default switchport	Displays default values for switch port attributes.

system default interface congestion timeout

To configure the default timeout value for a congestion timeout, use the **systemdefault interface congestion timeout** command. To disable this feature, use the **no** form of this command.

system default interface congestion timeout *milliseconds* **mode** {**core** | **edge**}
no system default interface congestion timeout *milliseconds* **mode** {**core** | **edge**}

Syntax Description

milliseconds	Number of milliseconds. The range is from 100 to 1000 milliseconds.
mode	Specifies the mode.
core	Specifies the core port type.
edge	Specifies the edge port type.

Command Default

500 milliseconds.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

When you set a smaller timeout on the edge ports such as 100 or 200 milliseconds the congestion on the edge port is reduced by making the packets on that port time out sooner when they see the pause condition.

Note You should use the default configuration for core ports and a value that does not exceed 500 ms (100 to 200 ms preferably) for fabric edge ports.

Examples

The following example shows how to configure the default value for a congestion timeout for the core port type:

```
switch# config terminal
switch(config)# system default interface congestion timeout 100 mode core
switch(config)#
```

The following example shows how to disable the default value for a congestion timeout for the edge port type:

```
switch# config terminal
switch(config)# system default interface congestion timeout 100 mode edge
switch(config)#
```

Related Commands

Command	Description
show interface brief	Displays FC port modes.
show system default switchport	Displays default values for switch port attributes.

system default interface pause mode

To configure the default timeout value for a pause frame, use the **systemdefault interfacepause mode** command. To disable this feature, use the **no** form of this command.

system default interface pause mode {**core** | **edge**}
no system default interface pause mode {**core** | **edge**}

Syntax Description

core	Specifies the core port type.
edge	Specifies the edge port type.

Command Default

None.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure the default timeout value for a pause frame for the core port type:

```
switch# config terminal
switch(config)# system default interface pause mode core
switch(config)#
```

The following example shows how to disable the timeout default value for a pause frame for the edge port type:

```
switch# config terminal
switch(config)# system default interface pause mode edge
switch(config)#
```

Related Commands

Command	Description
show interface brief	Displays FC port modes.
show system default switchport	Displays default values for switch port attributes.

system default interface pause timeout

To configure the default timeout value for a pause frame, use the **system defaultinterface pause timeout** command. To disable this feature, use the **no** form of the command.

system default interface pause timeout *milliseconds* **mode** {**core** | **edge**}
no system default interface pause timeout *milliseconds* **mode** {**core** | **edge**}

Syntax Description

milliseconds	Number of milliseconds. The range is from 100 to 500 milliseconds.
mode	Specifies the mode.
core	Specifies the core port type.
edge	Specifies the edge port type.

Command Default

500 milliseconds.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

When the port is in the state for the configured period, pause frame timeout can be enabled on that port. All frames that are sent to that port are dropped in the egress. This action frees up the buffer space in the ISL link (which carries traffic for this port) and helps to reduce congestion on other unrelated flows that use the same link.

Examples

The following example shows how to configure the timeout value pause frame for the core port type:

```
switch# config terminal
switch(config)# system default interface pause timeout 100 mode core
switch(config)#
```

The following example shows how to disable the timeout value pause for the edge port type:

```
switch# config terminal
switch(config)# system default interface pause timeout 100 mode edge
switch(config)#
```

Related Commands

Command	Description
show system default switchport	Displays default values for switch port attributes.

system default rib ipfc-mcast-deny

To configure the default behavior for an Internet protocol over Fibre Channel (IPFC) Multicast frame, use the **system default rib ipfc-mcast-deny** command in global configuration mode. To disable/remove the default configurations, use the **no** form of the command.

system default rib ipfc-mcast-deny
no system default rib ipfc-mcast-deny

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled. The system will allow the IPFC multicast traffic on F-ports.

Command Modes

Global Configuration mode.

Command History

Release	Modification
8.4(1)	This command was introduced.

Usage Guidelines

The **system default rib ipfc-mcast-deny** command can be used only when the host devices are registered as IPFC type to the switch.

Examples

The following example shows how to enable the **system default rib ipfc-mcast-deny** command:

```
switch# config terminal
switch(config)# system default rib ipfc-mcast-deny
```

The following example shows how to view the status of the **system default rib ipfc-mcast-deny** command:

```
switch# show system default rib

switch# system default rib ipfc-mcast-deny enabled
```

Related Commands

Command	Description
show system default rib	Displays the **system default rib ipfc-mcast-deny** command status.

system default switchport

To configure port attributes, use the**system default switchport** command in configuration mode. To disable port attributes, use the **no** form of the command.

system default switchport {**shutdown** | **trunk mode** {**auto** | **off** | **on**} | **mode** { **auto-sw-3** | **F** } }
no system default switchport {**shutdown** | **trunk mode** {**auto** | **off** | **on**} | **mode** { **auto-sw-3** | **F** } }

Syntax Description

shutdown	Disables or enables switch ports by default.
trunk	Configures the trunking parameters as a default.
mode	Configures the trunking mode.
auto	Enables autosense trunking.
off	Disables trunking.
on	Enables trunking.
mode auto-sw-3	Sets the error detection timeout value to 6 seconds. By default, this value is 2 seconds.
mode F	Sets the administrative mode of Fibre Channel ports to mode F.

Command Default

Enabled.

Command Modes

Configuration mode

Command History

Release	Modification
9.2(1)	Added the **auto-sw-3** option.
3.1(3)	Added the **mode F** option.
1.0(2)	This command was introduced.

Usage Guidelines

Attributes configured using this command are applied globally to all future switch port configurations, even if you do not individually specify them at that time.

This command changes the configuration of the following ports to administrative mode F:

- All ports that are down.
- All F ports that are up, whose operational mode is F, and whose administrative mode is not F.

This command does not affect non-F ports that are up; however, if non-F ports are down, this command changes the administrative mode of those ports.

Examples

The following example shows how to configure port shutdown:

```
switch# config terminal
switch(config)# system default switchport shutdown
```

The following example shows how to configure the trunk mode:

```
switch# config terminal
switch(config)# system default switchport trunkmode auto
```

The following example shows how to set the administrative mode of Fibre Channel ports to mode F:

```
switch# config terminal
switch(config)# system default switchport mode F
```

The following example shows how to set the administrative mode of Fibre Channel ports to the default:

```
switch# config terminal
switch(config)# no system default switchport mode F
```

The following example shows how to set the error detection timeout value to 6 seconds:

```
switch# config terminal
switch(config)# system default switchport mode auto-sw-3
```

Related Commands

Command	Description
show interface brief	Displays FC port modes.
show system default switchport	Displays default values for switch port attributes.

system-default-tx-credits-double-queue

To configure TX credit queue as double queue, use the **system default tx-credit double-queue** command. To revert to the default TX credit queue, use the **no** form of this command.

system default tx-credit double-queue

Command Default

TX credit queue is configured as single queue.

Command Modes

Configuration mode (config)

Command History

Release	Modification
5.2(6)	This command was introduced.

Examples

The following example displays how to configure the TX credit queue as double queue:

```
switch# configure terminal
switch(config)# system default tx-credit double-queue
```

The following example displays how to return to the default TX credit queue:

```
switch# configure terminal
switch(config)# no system default tx-credit double-queue
```

Related Commands

Command	Description
show system	Displays the system information.

system default zone default-zone permit

To configure default values for a zone, use the **system default zone default-zone permit** command in configuration mode. To revert to the defaults, use the **no** form of the command.

system default zone default-zone permit
no system default zone default-zone permit

Syntax Description

This command has no arguments or keywords.

Command Default

No default values for zones.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command defines the default values for the default zone for all VSANs. The default values are used when you initially create a VSAN and it becomes active. If you do not want to use the default values, use the **zone default-zone permit vsan** command to define the operational values for the default zone.

The **system default zone default-zone permit** command should only be used in conjunction with VSANs that have not yet been created; it has no effect on existing VSANs.

Note Because VSAN 1 is the default VSAN and is always present, this command has no effect on it.

Examples

The following example sets the default zone to use the default values:

```
switch# config terminal
switch(config)# system default zone default-zone permit
```

The following example restores the default setting:

```
switch(config)# no
 system default zone default-zone permit
```

Related Commands

Command	Description
show system default zone	Displays default values for the default zone.
zone default-zone permit vsan	Defines whether a default zone (nodes not assigned a created zone) permits or denies access to all in the default zone.

system default zone distribute full

To configure default values for distribution to a zone set, use the **system default zone distribute full** command in configuration mode. To revert to the defaults, use the **no** form of the command.

system default zone distribute full
no system default zone distribute full

Syntax Description

This command has no arguments or keywords.

Command Default

Distribution to active zone sets only.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command distributes the default values for the default zone to all VSANs. The default values are used when you initially create a VSAN and it becomes active. If you do not want to use the default values, use the **zoneset distribute full vsan** command to distribute the operational values for the default zone.

The **system default zone distribute full** command should only be used in conjunction with VSANs that have not yet been created; it has no effect on existing VSANs.

Note Because VSAN 1 is the default VSAN and is always present, this command has no effect on it.

Examples

The following example distributes default values to the full zone set:

```
switch# config terminal
switch(config)# system default zone distribute full
```

The following example distributes default values to the active zone set only:

```
switch(config)# no
 system default zone distribute full
```

Related Commands

Command	Description
show system default zone	Displays default values for the default zone.
zoneset distribute full vsan	Distributes the operational values for the default zone to all zone sets.

system default zone gs

To configure default value for zone generic service permission, use the **system default zone gs** command in the configuration mode. To set the default value for zone generic service permission as none (deny), use the no form of the command.

system default zone gs {**read** | **read-write**}
no system default zone gs {**read** | **read-write**}

Syntax Description

read	Specifies the default zone generic service permission as read.
read-write	Specifies the default zone generic service permission as read-write.

Command Default

read-write.

Command Modes

Configuration mode

Command History

Release	Modification
3. 2(1)	This command was introduced.

Usage Guidelines

Setting write only as the default value for zone generic service permission is not supported.

Examples

The following example shows how to configure the default value for zone generic service permission as read only for new VSANs:

```
switch# config terminal
switch(config)# system default zone gs read
switch(config)#
```

The following example shows how to configure the default value for zone generic service permission as read-write for new VSANs:

```
switch# config terminal
switch(config)# system default zone gs read-write
switch(config)#
```

The following example shows how to configure the default value for zone generic service permission as none (deny) for new VSANs:

```
switch# config terminal
switch(config)# no system default zone gs read-write
switch(config)#
```

Related Commands

Command	Description
show system default zone	Displays the zone specific system default value settings.

system default zone mode enhanced

To configure the zone mode default value as enhanced, use the **system default zone mode enhanced** command in the configuration mode. To configure the zone mode default value as basic, use the no form of the command.

system default zone mode enhanced
no system default zone mode enhanced

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

This command configures the default value of zoning mode as basic or enhanced. The default value of zoning mode is used when a VSAN is newly created. If the VSAN is deleted and recreated, the value of the zoning mode defaults to the value specified by the configuration.

Examples

The following example shows how to configure the zone mode default value as enhanced:

```
switch# config
switch# system default zone mode enhanced
```

The following example shows how to configure the zone mode default value as basic:

```
switch# config
switch# no system default zone mode enhanced
```

Related Commands

Command	Description
show system default zone	Displays the default value of zone mode as basic and enhanced.

system default zone smart-zone

To configure the default values for smart zone, use the system default zone smart-zone command in the configuration mode. To disable this feature, use the no form of the command.

system default zone smart-zone enable
no system default zone smart-zone enable

Syntax Description

enable	Specifies the default smart zone enable or disable.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure the default values for smart-zone :

```
switch# config
switch(config)# no system default zone smart-zone enable
switch(config)#
```

Related Commands

Command	Description
show system default zone	Displays the default value of zone mode as basic and enhanced.

system delayed-traps enable mode

To configure the system-delayed trap state, use the **system delayed-traps enable** mode command. To disable the system-delayed trap state, use the **no** form of the command.

system delayed-traps enable mode FX
no system delayed-traps enable mode FX

Syntax Description

FX	Enables or disables delayed traps for operationally up FX (F/FX) mode interfaces.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the system-delayed trap state:

```
switch(config)# system delayed-traps enable mode FX
switch(config)#
```

system delayed-traps timer

To configure the system-delayed trap timeout values, use the **system delayed-traps timer** command. To disable the system-delayed trap timeout values, use the **no** form of the command.

system delayed traps-timer *number*
no system delayed traps-timer *number*

Syntax Description

number	Indicates the delayed trap timer in minutes. The range is from 1 to 60.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

System delayed traps timer is optional. If the user does not provide the timer value, default value of 4 is applied.

Examples

The following example shows how to configure system-delayed trap values:

```
switch(config)# system delayed-traps timer 30
switch(config)#
```

system hap-reset

Command	Description
show system default zone	Displays the default value of zone mode as basic and enhanced.

To configure the HA reset policy, use the **system hap-reset** command in EXEC mode. Use the **no** form of this command to disable this feature.

system hap-reset
system no hap-reset

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can disable the HA policy supervisor reset feature (enabled by default) for debugging and troubleshooting purposes.

Examples

The following example enables the supervisor reset HA policy:

```
switch# system hap-reset
```

system health (configuration mode)

To configure Online Health Management System (OHMS) features for a specified interface or for the entire switch, use the **system health** command. To disable this feature, use the **no** form of the command.

system health [**failure-action** | **interface** {**fc** *slot/port* | **iscsi** *slot/port*} | **loopback** {**frame-length** { *bytes* | **auto**} | **frequency** *seconds*}]
no system health [**failure-action** | **interface** {**fc** *slot/port* | **iscsi** *slot/port*}]



Note On a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter, the syntax differs as follows:**interface bay** *port* | **ext** *port* }

Syntax Description

failure-action	(Optional) Prevents the NX-OS software from taking any OHMS action for the entire switch.
interface	(Optional) Configures an interface.
fc *slot*/*port*	(Optional) Specifies the Fibre Channel interface to configure by slot and port number on an MDS 9000 Family switch.
iscsi *slot*/*port*	(Optional) Specifies the iSCSI interface to configure by slot and port number on an MDS 9000 Family switch.
bay *port* | ext *port*	(Optional) Configures the Fibre Channel interface on a port on a Cisco Fabric Switch for HP c-Class BladeSystem or on a Cisco Fabric Switch for IBM BladeCenter. The range is 0 to 48.
loopback	(Optional) Configures the OHMS loopback test.
frame-length *bytes*	(Optional) Specifies the frame-length in bytes ranging from 0 to 128 bytes for the loopback test.
auto	(Optional) Configures the frame-length to auto for the loopback test.
frequency *seconds*	(Optional) Specifies the loopback frequency in seconds ranging from 5 seconds (default) to 255 seconds.

Command Default

Enabled.

Frame-length is auto-size, which could range from 0 to 128.

Command Modes

Configuration mode

Command History

Release	Modification
1.3(4)	This command was introduced.
3.0(1)	Added the **frame-length** and **auto** options to the **loopback** keyword.

Release	Modification
3.1(2)	Added the **interface bay | ext** option.

Usage Guidelines

If you do not configure the loopback frequency value, the default frequency of 5 seconds is used for all modules in the switch.



Note The **no** form of the command is not supported for the **frame-length**, **auto**, and **frequency** options.

Examples

The following example disables OHMS in this switch:

```
switch# config terminal
switch(config)# no system health
System Health is disabled.
```

The following example enables (default) OHMS in this switch:

```
switch(config)# system health
System Health is enabled.
```

The following example enables OHMS in this interface:

```
switch(config)# no system health interface fc8/1
System health for interface fc8/13 is enabled.
```

The following example disables OHMS in this interface:

```
switch(config)# system health interface fc8/1
System health for interface fc8/13 is disabled.
```

The following example configures the loopback frequency to be 50 seconds for any port in the switch:

```
switch(config)# system health loopback frequency 50
The new frequency is set at 50 Seconds.
The following example configures the loopback frame-length to auto:
switch(config)# system health loopback frame-length auto
Loopback frame-length auto-size mode is now enabled.
```

The following example prevents the switch from taking any failure action:

```
switch(config)# system health failure-action
System health global failure action is now enabled.
```

The following example prevents the switch configuration from taking OHMS action (default) in case of a failure:

```
switch(config)# no system health failure-action
System health global failure action now disabled.
```

Related Commands

Command	Description
system health external-health	Explicitly runs an external Online Health Management System (OHMS) loopback test on demand for a specified interface or module.
system health internal-loopback	Explicitly runs an internal OHMS loopback test on demand for a specified interface or module.
system health serdes-loopback	Explicitly runs an internal OHMS Serializer/Deserializer (Serdes) loopback test on demand for a Fibre Channel interface.

system health cf-crc-check

To run the CompactFlash CRC checksum test on demand, use the **system health cf-crc-check** command in EXEC mode.

system health cf-crc-check module *slot*

Syntax Description

module*slot*	Specifies the module slot number.

Command Default

Enabled to automatically run in the background every 7 days.

Command Modes

EXEC mode

Command History

Release	Modification
3.1(3)	This command was introduced.

Usage Guidelines

Run the CompactFlash CRC checksum test on demand to determine if the CompactFlash firmware is corrupted and needs to be updated.

The CRC checksum test can be run on demand on the following modules:

- DS-X9016
- DS-X9032
- DS-X9302-14K9
- DS-X9308-SMIP
- DS-X9304-SMIP
- DS-X9530-SF1-K9

Examples

The following example shows how to run the CRC checksum test on demand:

```
switch# system health cf-crc-check module 4
```

Related Commands

Command	Description
show system health	Displays system health information.
show system health statistics	Displays system health statistics.

system health cf-re-flash

To update the CompactFlash firmware on demand, use the **system health cf-re-flash** command in EXEC mode.

system health cf-re-flash module *slot*

Syntax Description

module*slot*	Specifies the module slot number.

Command Default

Enabled to automatically run in the background every 30 days.

Command Modes

EXEC mode

Command History

Release	Modification
3.1(3)	This command was introduced.

Usage Guidelines

The CRC checksum test and the firmware update can be enabled on the following modules:

- DS-X9016
- DS-X9032
- DS-X9302-14K9
- DS-X9308-SMIP
- DS-X9304-SMIP
- DS-X9530-SF1-K9

Examples

The following example shows how to update firmware on demand:

```
switch# system health cf-re-flash module 4
```

Related Commands

Command	Description
show system health	Displays system health information.
show system health statistics	Displays system health statistics.

system health clear-errors

To clear previous error conditions stored in the Online Health Management System (OHMS) application's memory, use the **system health clear-errors** command.

system health clear-errors interface {**fc slotport** | **iscsi slotport**}
system health clear-errors module *slot* [**battery-charger** | **bootflash** | **cache-disk** | **eobc** | **inband** | **loopback** | **mgmt**]



Note On a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter, the syntax differs as follows:**interface bay** *port* **| ext** *port* }

Syntax Description

interface	Specifies the interface to be configured.
fc *slot*/*port*	Configures the Fiber Channel interface on a Cisco MDS 9000 Family switch.
iscsi *slot*/*port*	Selects the iSCSI interface to configureon a Cisco MDS 9000 Family switch.
bay *port* **| ext** *port*	(Optional) Configures the Fibre Channel interface on a port on a Cisco Fabric Switch for HP c-Class BladeSystem or on a Cisco Fabric Switch for IBM BladeCenter.
module *slot*	Specifies the required module in the switch,
battery-charger	(Optional) Configures the OHMS battery-charger test on the specified module
bootflash	(Optional) Configures the OHMS bootflash test on the specified module.
cache-disk	(Optional) Configures the OHMS cache-disk test on the specified module.
eobc	(Optional)Configures the OHMS EOBC test on the specified module.
inband	(Optional) Configures the OHMS inband test on the specified module.
loopback	(Optional) Configures the OHMS loopback test on the specified module.
mgmt	(Optional) Configures the OHMS management port test on the specified module.

Command Default

Enabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.
3.1(2)	Added the **interface bay | ext** option.

Usage Guidelines

You can clear the error history for Fibre Channel interfaces, iSCSI interfaces, for an entire module, or one particular test for an entire module. The **battery-charger**, the **bootflash**, the **cache-disk**, the **eobc**, the **inband**, the **loopback**, and the **mgmt** test options can be individually specified for a given module.

The management port test cannot be run on a standby supervisor module.

Examples

The following example clears the error history for the specified Fibre Channel interface:

```
switch# system health clear-errors interface fc 3/1
```

The following example clears the error history for the specified module:

```
switch# system health clear-errors interface module 3
```

The following example clears the management port test error history for the specified module:

```
switch# system health clear-errors module 2 mgmt
```

system health external-loopback

To explicitly run an external Online Health Management System (OHMS) loopback test on demand (when requested by the user) for a specified interface or module, use the **system health external-loopback** command.

system health external-loopback {**interface fc** *slot/port* | **source interface fc** *slot/port* **destination fc** *slot/port*} [**frame-length** *bytes* [**frame-count** *number*] | **frame-count** *number*] [**force**]



Note On a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter, the syntax differs as follows:**interface bay** *port* **| ext** *port* }

Syntax Description

interface	Configures an interface.
fc *slot*/*port*	Configures the Fibre Channel interface specified by the slot and port on an MDS 9000 Family switch.
source	Specifies the source Fibre Channel interface.
destination	Specifies the destination Fibre Channel interface.
bay | **ext** port	(Optional) Configures the Fibre Channel interface on a Cisco Fabric Switch for HP c-Class BladeSystem or on a Cisco Fabric Switch for IBM BladeCenter . The range is 0 to 48.
frame-length *bytes*	(Optional) Configures the specified length of the loopback test frame in bytes. The range is 0 to 128 bytes.
frame-count *number*	(Optional) Configures the specified number of frames for the loopback test. The number of frames can range from 1 to 32.
force	(Optional) Directs the software to use the non-interactive loopback mode.

Command Default

The loopback is disabled.

The frame-length is 0. The frame-count is 1.

Command Modes

EXEC mode

Command History

Release	Modification
1.3(4)	This command was introduced.
3.0(1)	Added the **source** and **destination** keywords and the **frame-count** and **frame-length** options.
3.1(2)	Added the **interface bay** | **ext** option.

Usage Guidelines

Use this command to run this test on demand for the external devices connected to a switch that are part of a long haul network.

Examples

The following example displays an external loopback command for a Fibre Channel interface:

```
switch# system health external-loopback interface fc 3/1
This will shut the requested interfaces Do you want to continue (y/n)? [n] y
External loopback test on interface fc3/1 was  successful.
```

The following example displays the effect of the **force** option when implementing a forced loopback:

```
switch# system health external-loopback interface fc 3/1 force
External loopback test on interface fc3/1 was  successful.
```

Related Commands

Command	Description
system health	Configures Online Health Management System (OHMS) features for a specified interface or for the entire switch.
system health internal-loopback	Explicitly runs an internal OHMS loopback test on demand for a specified interface or module.
system health serdes-loopback	Explicitly runs an internal OHMS Serializer/Deserializer (Serdes) loopback test on demand for a Fibre Channel interface.

system health internal-loopback

To explicitly run an internal Online Health Management System (OHMS) loopback test on demand (when requested by the user) for a specified interface or module, use the **system health internal-loopback** command.

system health internal-loopback interface {**fc slot/port** | **iscsi slot**/**port**} [**frame-length bytes** [**frame-count number**] | **frame-count number**]

Note On a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter, the syntax differs as follows:**interface [bay** *port* **| ext** *port]*

Syntax Description

interface	Configures an interface.
fc *slot*/*port*	Configures the Fibre Channel interface specified by the slot and port on an MDS 9000 Family switch.
iscsi *slot*/*port*	Specifies the iSCSI interface to configure by slot and port on an MDS 9000 Family switch.
bay *port* **| ext** *port*	(Optional) Configures the Fibre Channel interface on a Cisco Fabric Switch for HP c-Class BladeSystem or on a Cisco Fabric Switch for IBM BladeCenter . The range is 0 to 48.
frame-length *bytes*	(Optional) Configures the specified length of the loopback test frame in bytes. The range is 0 to 128 bytes.
frame-count *number*	(Optional) Configures the specified number of frames for the loopback test. The number of frames can range from 1 to 32.

Command Default

The loopback is disabled.

The frame-length is 0. The frame-count is 1.

Command Modes

EXEC mode

Command History

Release	Modification
1.3(4)	This command was introduced.
3.0(1)	Added the **frame-count** and **frame-length** options.
3.1(2)	Added the **interface bay	ext** option.

Usage Guidelines

Internal loopback tests send and receive FC2 frames to and from the same ports and provide the round trip time taken in microseconds for the Fibre Channel interface.

Examples

The following example performs the internal loopback test for a Fibre Channel interface:

```
switch# system health internal-loopback interface iscsi 8/1
Internal loopback test on interface iscsi 8/1 was successful.
Round trip time taken is 79 useconds
```

Related Commands

Command	Description
system health	Configures Online Health Management System (OHMS) features for a specified interface or for the entire switch.
system health external-loopback	Explicitly runs an external OHMS loopback test on demand for a specified interface or module.
system health serdes-loopback	Explicitly runs an internal OHMS Serializer/Deserializer (Serdes) loopback test on demand for a Fibre Channel interface.

system health module

To configure Online Health Management System (OHMS) features for a specified module, use the **system health module** command. To disable these features, use the **no** form of this command.

system health module *slot* [**battery-charger** [**failure-action** | **frequency** *seconds*] | **bootflash** [**failure-action** | **frequency** *seconds*] | **cache-disk** [**failure-action** | **frequency** *seconds*] | **cf-crc-check** [**failure-action** | **frequency** *frequency*] | **cf-re-flash** [**failure-action** | **frequency** *frequency*] | **eobc** [**failure-action** | **frequency** *seconds*] | **failure-action** | **inband** [**failure-action** | **frequency** *seconds*] | **loopback** [**failure-action**] | **mgmt** [**failure-action** | **frequency** *seconds*]]
no system health module *slot* [**battery-charger** [**failure-action** | **frequency** *seconds*] | **bootflash** [**failure-action** | **frequency** *seconds*] | **cache-disk** [**failure-action** | **frequency** *seconds*] | **cf-crc-check** [**failure-action** | **frequency** *frequency*] | **cf-re-flash** [**failure-action** | **frequency** *frequency*] | **eobc** [**failure-action** | **frequency** *seconds*] | **failure-action** | **inband** [**failure-action** | **frequency** *seconds*] | **loopback** [**failure-action**] | **mgmt** [**failure-action** | **frequency** *seconds*]]

Syntax Description

slot	The module slot number.
battery-charger	(Optional) Configures the battery-charger test on the specified module.
failure-action	(Optional) Controls the software from taking any action if a CompactFlash failure is determined while running the CRC checksum test.
frequency *seconds*	(Optional) Specifies the frequency in seconds. The range for the **bootflash frequency** option is 10 to 255. The range for the **cf-crc-check frequency** option is 1 to 30. The range for the **cf-re-flash frequency** option is 30 to 90. For all other options, the range is 5 to 255.
bootflash	Configures the bootflash test on the specified module.
cache-disk	Configures the cache-disk test on the specified module.
cf-crc-check	Configures the CRC checksum test.
cf-re-flash	Configures the firmware update.
eobc	Configures the EOBC test on the specified module.
inband	Configures the inband test on the specified module.
loopback	Configures the loopback test on the specified module.
mgmt	Configures the management port test on the specified module.

Command Default

The default for OHMS is enabled.

The CRC Checksum test is enabled to automatically run in the background every 7 days.

The firmware update is enabled to automatically run in the background every 30 days.

The **failure-action** feature is enabled.

Command Modes

Configuration mode

Command History

Release	Modification
1.3(4)	This command was introduced.
3.1(3)	Added the **cf-crc-check** and **cf-reflash** options.

Usage Guidelines

The CRC checksum test and the firmware update can be enabled on the following modules:

- DS-X9016
- DS-X9032
- DS-X9302-14K9
- DS-X9308-SMIP
- DS-X9304-SMIP
- DS-X9530-SF1-K9

If you do not configure the loopback frequency value, the default frequency of 5 seconds is used for all modules in the switch.

Examples

The following example enables the battery-charger test on both batteries in the CSM module. If the switch does not have a CSM, this message is issued:

```
switch# config terminal
switch(config)# system health module 6 battery-charger
battery-charger test is not configured to run on module 6.
```

The following example enables the cache-disk test on both disks in the CSM module. If the switch does not have a CSM, this message is issued:

```
switch(config)# system health module 6 cache-disk
cache-disk test is not configured to run on module 6.
```

The following example enables the bootflash test:

```
switch(config)# system health module 6 bootflash
System health for module 6 Bootflash is already enabled.
```

The following example enables you to prevent the NX-OS software from taking any action if any component fails:

```
switch(config)# system health module 6 bootflash failure-action
System health failure action for module 6 Bootflash test is now enabled.
```

The following example enables an already-enabled bootflash test:

```
switch(config)# system health module 6 bootflash failure-action
System health failure action for module 6 Bootflash test is already enabled.
```

The following example disables the bootflash test configuration:

```
switch(config)# no system health module 6 bootflash failure-action
System health failure action for module 6 Bootflash test is now disabled.
```

The following example sets the new frequency of the bootflash test to 200 seconds:

```
switch(config)# system health module 6 bootflash frequency 200
The new frequency is set at 200 Seconds.
```

The following example enables the EOBC test:

```
switch(config)# system health module 6 eobc
System health for module 6 EOBC is now enabled.
```

The following example enables the inband test:

```
switch(config)# system health module 6 inband
System health for module 6 EOBC is now enabled.
```

The following example enables the loopback test:

```
switch(config)# system health module 6 loopback
System health for module 6 EOBC is now enabled.
```

The following example enables the management test:

```
switch(config)# system health module 6 management
System health for module 6 EOBC is now enabled.
```

The following example shows how to set the CompactFlash CRC test interval:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# system health module 6 cf-crc-check frequency 10
```

The following example shows how to set the CompactFlash CRC test **failure-action** feature:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# system health module 6 cf-crc-check failure-action
```

The following example shows how to set the CompactFlash reflash update interval:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# system health module 6 cf-reflash frequency 10
```

The following example shows how to set the CompactFlash reflash **failure-action** feature:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# system health module # cf-re-flash failure-action
```

Related Commands

Command	Description
show system health	Displays system health information.
show system health statistics	Displays system health statistics.

system health serdes-loopback

To explicitly run an internal Online Health Management System (OHMS) Serializer/Deserializer (Serdes) loopback test on demand (when requested by the user) for a Fibre Channel interface, use the **system health serdes-loopback** command.

system health serdes-loopback interface fc *slot/port* [**frame-length** *bytes* [**frame-count** *number*] | **frame-count** *number*] [**force**]

Syntax Description



Note On a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter, the syntax differs as follows:**interface bay** *port* **| ext** *port* }

interface	Configures an interface.
fc *slot*/*port*	(Optional) Configures the Fiber Channel interface specified by the slot and port on an MDS 9000 Family switch.
bay *port* **| ext** *port*	(Optional) Configures the Fibre Channel interface on a Cisco Fabric Switch for HP c-Class BladeSystem or on a Cisco Fabric Switch for IBM BladeCenter. The range is 0 to 48.
force	Directs the software to use the non-interactive loopback mode.
frame-length *bytes*	(Optional) Configures the specified length of the loopback test frame in bytes. The range is 0 to 128 bytes.
frame-count *number*	(Optional) Configures the specified number of frames for the loopback test. The number of frames can range from 1 to 32.

Command Default

Loopback is disabled.

The frame-length is 0. The frame-count is 1.

Command Modes

EXEC mode

Command History

Release	Modification
3.0(1)	This command was introduced.
3.1(2)	Added the **interface bay | ext** option**.**

Usage Guidelines

None.

Examples

The following example performs a Serdes loopback test within ports for an entire module:

```
switch# system health serdes-loopback interface fc 4/1
```

This will shut the requested interfaces Do you want to continue (y/n)? [n] y

```
Serdes loopback test on interface fc 4/1 was successful.
```

The following example performs a Serdes loopback test within ports for the entire module and overrides the frame count configured on the switch:

```
switch# system health serdes-loopback interface fc 3/1 frame-count 10
This will shut the requested interfaces Do you want to continue (y/n)? [n] y
Serdes loopback test passed for module 3 port 1
```

Related Commands

Command	Description
system health	Configures Online Health Management System (OHMS) features for a specified interface or for the entire switch.
system health external-loopback	Explicitly runs an external OHMS loopback test on demand for a specified interface or module.
system health internal-loopback	Explicitly runs an internal OHMS loopback test on demand for a specified interface or module.

system heartbeat

To enable system heartbeat checks, use the **system heartbeat** command in EXEC mode. Use the **no** form of this command to disable this feature.

system heartbeat
no system heartbeat

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can disable the heartbeat checking feature (enabled by default) for debugging and troubleshooting purposes such as attaching a GDB to a specified process.

Examples

The following example enables the system heartbeat checks:

```
switch# system heartbeat
```

system kernel core

To enable kernel core logging, use the **system kernel core** command. To disable this feature, use the **no** form of this command.

system kernel core
no system kernel core

Command Default

Kernel core logging is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
8.4(2c)	This command was introduced.

Usage Guidelines

Kernel core logging is supported only on Cisco MDS 9718, MDS 9710, and MDS 9706 switches.

Examples

This example shows how to enable kernel core logging:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# system kernel core
```

This example shows how to disable kernel core logging:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no system kernel core
```

Related Commands

Command	Description
show cores	Displays a list of core bundles in the switch core repository.

system memlog

To collect system memory statistics, use the **system memlog** command in EXEC mode.

system memlog

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use this command for debugging and troubleshooting purposes.

Examples

The following example enables system memory logging:

```
switch# system memlog
```

system port pacer mode F interface-login-threshold

To enable the pacer mode for F port threshold limit, use the **system port pacer mode F**

interface -login-threshold command.

system port pacer mode F interface-login-threshold *port-threshold limit* **concurrent-ports** *port-number*

Syntax Description

mode F	Specifies the F mode.
interface-login-threshold *port-threshold limit*	Specifies the per port threshold limit. The range is from 0 to 256.
concurrent-ports *port-number*	Specifies the maximum number of concurrent port bring up allowed. The range is from 1 to 16. Preferred value is 1.

Command Default

Disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
6.2(7)	This command was introduced.

Usage Guidelines

Note Concurrent-ports port-number needs to be set depending upon customers topology and tune this value onto how many F ports can be brought up simultaneously.

Note Fx or FL or E ports are not supported.

Examples

The following example shows how to enable the pacer mode F for port threshold limit:

```
switch(config)#
system port pacer mode F interface-login-threshold 10 concurrent-ports 1
switch(config)#
```

system startup-config

To release a system startup configuration lock, use the system startup-config**system startup config** command in EXEC mode.

system startup-config unlock *lock-id*

Syntax Description

unlock *lock-id*	Configures the system startup-config unlock ID number. The range is 0 to 65536.

Command Default

Disabled.

Command Modes

EXEC

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

The **system startup-config** command allows you to unlock or release the rr_token lock. To determine the *lock-id, use the* **show system internal sysmgr startup-config locks** command.

Examples

The following example releases the system configuration lock with identifier 1:

```
switch# system ?
  hap-reset       Enables resetting of local or remote sup on ha failures
  health          System health exec commands
  heartbeat       Enables heartbeat
  memlog          Generate memory log in bootflash
  no              Negate a command or set its defaults
  pss             PSS commands
  standby         System standby manual boot
  startup-config  System startup-config commands
  statistics      Changes statistics configuration
  switchover      Switchover now
  watchdog        Enables watchdog
switch# system startup-config ?
  unlock  Unlock startup-config
switch# system startup-config unlock ?
  <0-65536>  Startup-config lock id
switch# system startup-config unlock 1 ?
  <cr>  Carriage Return
switch# system startup-config unlock 1
```

Related Commands

Command	Description
show system	Displays system information.

system statistics reset

To reset the high availability statistics collected by the system, use the **system statistics reset** command in EXEC mode.

system statistics reset

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can disable the system statistics reset feature (enabled by default) for debugging and troubleshooting purposes.

Examples

The following example resets the HA statistics:

```
switch# system statistics reset
```

system switchover (configuration mode)

To enable a switchover for the system, use the **system switchover** command in configuration mode. To revert to the factory default setting, use the **no** form of the command.

system switchover {**ha** | **warm**}
no system switchover

Syntax Description

ha	Specifies an HA switchover.
warm	Specifies a warm switchover.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables a HA switchover from an active supervisor module to a standby supervisor module:

```
switch# config terminal
switch(config)# system switchover ha
```

system switchover (EXEC mode)

To specifically initiate a switchover from an active supervisor module to a standby supervisor module, use the**system switchover** command in EXEC mode.

system switchover bypass-standby-mgmt0

Syntax Description

bypass-standby-mgmt0	Specifies to bypass the standby supervisor's mgmt0 interface status check before performing a switchover.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
9.2(1)	The **bypass-standby-mgmt0** keyword was introduced.
1.3(1)	This command was introduced.

Usage Guidelines

Starting with Cisco MDS NX-OS Release 9.2(1), the **system switchover** command checks the status of the mgmt0 link on the standby supervisor of the Cisco MDS 9700 directors with dual supervisors. If the standby supervisor is not up, then the system switchover will not proceed and displays an error. This is to prevent the switch from losing out of band management access. To bypass this check use the **bypass-standby-mgmt0** option that is also available from Cisco MDS NX-OS Release 9.2(1).

Examples

The following example initiates a HA switchover from an active supervisor module to a standby supervisor module:

```
switch# system switchover
```

The following message is displayed when you try to perform a switchover to the standby supervisor when the **bypass-standby-mgmt0** option was not used and the standby supervisor's mgmt0 interface was down:

```
System switchover not allowed when standby supervisor mgmt0 link is down. Use the
bypass-standby-mgmt0 parameter to bypass this check and force switchover to standby
supervisor.
```

Related Commands

Command	Description
show module	Displays the HA-standby state for the standby supervisor module.
show system redundancy status	Determines whether the system is ready to accept a switchover.
show version compatibility	Determines version compatibility between switching modules.

system timeout congestion-drop

To configure the system timeout values for congestion drop, use the **system timeout congestion-drop** command.

system timeout congestion-drop *number* **logical-type** {**core** | **edge}** | **default logical-type** {**core** | **edge}**

Syntax Description

number	Number in milliseconds. The range is from 200 ms to 500 ms. The congestion timeout value should be in multiples of 10.
default	Specifies the default timeout values for congestion drop.
logical-type	Specifies the logical type for a port.
core	Specifies the core mode.
edge	Specifies the edge mode.

Command Default

The default system timeout congestion-drop value is 500 ms.

Command Modes

Global configuration mode

Command History

Release	Modification
8.1(1)	• **mode** keyword was change to **logical-type** keyword, **E** keyword was changed to **core** keyword, and **F** keyword was changed to **edge** keyword. • The system timeout congestion-drop value range was changed from 100-500 ms to 200-500 ms.
4.2(7a)	This command was introduced.

Usage Guidelines

Each packet received by the MDS is timestamped. This timer determines hold long the MDS holds packets to transmit. If the timer expires then the packet is discarded as a timeout frame.

Examples

The following example shows how to configure the system timeout values for congestion drop core mode:

```
switch# configure terminal
switch(config)# system timeout congestion-drop 210 logical-type core
```

The following example shows how to configure the default timeout values for congestion drop core mode:

```
switch(config)# system timeout congestion-drop default logical-type core
```

Related Commands

Command	Description
system timeout no-credit-drop	Configures the system timeout values for no credit drop.

system timeout no-credit-drop

To configure the system timeout values for no credit drop, use the **system timeout no-credit-drop** command. To disable the system timeout values, use the **no** form of this command.

{**system timeout no-credit-drop** *number* **logical-type edge** | **default logical-type edge**}
{**no system timeout no-credit-drop** *number* **logical-type edge** | **default logical-type edge**}

Syntax Description

number	Number in milliseconds. The range is from 1 to 500 milliseconds.
default	Specifies the default timeout values for no credit drop. The default value is 500 milliseconds.
logical-type	Specifies the logical type for a port.
edge	Specifies the edge mode.

Command Default

By default, frame dropping is disabled and the frame timeout value is 500 ms for all port types.

Command Modes

Global configuration mode

Command History

Release	Modification
8.1(1)	**mode** keyword was change to **logical-type** keyword, and **F** keyword was changed to **edge** keyword.
6.2(9)	Changed the **no-credit-drop** timeout value.
4.2(7a)	This command was introduced.

Usage Guidelines

This timer, when enabled, determines how long an interface is at zero Tx buffer to buffer credits before it starts dropping packets immediately and not waiting for the congestion-drop timeout.

Note **no-credit- drop** timeout value has been changed from 100 to 500 in multiples of 100 milliseconds. Current range changes from 1 to 500 in multiples of 1 milliseconds.

Examples

The following example shows how to configure the system timeout values for no credit drop edge mode:

```
switch(config)# system timeout no-credit-drop 100 logical-type edge
```

The following example shows how to configure the default timeout values for no credit drop edge mode:

```
switch(config)# system timeout no-credit-drop default logical-type edge
```

The following example shows how to disable the system timeout value for no credit drop edge mode:

```
switch(config)# no system timeout no-credit-drop default logical-type edge
```

Related Commands

Command	Description
system timeout congestion-drop	Configures the system timeout values for congestion drop.

system timeout slowport-monitor

To configure the system timeout values for hardware slowport monitoring, use the **system timeout slowport-monitor** command. To remove this feature, use the **no** form of this command.

system timeout slowport-monitor *number* **default mode E/F**
no system timeout slowport-monitor *number* **default mode E/F**

Syntax Description

number	Number in milliseconds. The range is from 1 to 500 milliseconds.
default	Specifies the default timeout value for the hardware slowport monitoring. The default value is 50 milliseconds.
mode	Specifies the Port mode.
E	Specifies the E port mode.
F	Specifies the F port mode.

Command Default

Disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
6.2(9)	This command was introduced.

Usage Guidelines

This timer, when enabled, starts the slowport monitoring of ports and collects the statistics information like average credit delay and the number of times slowport event detected count.

This command is applicable for the platforms that support hardware slowport monitoring (MDS 9710, 9706,9250i,9148S).

Examples

The following example shows how to configure the system timeout values for hardware slowport monitoring:

```
switch(config)# system timeout slowport-monitor 10 mode F
switch(config)#
```

The following example shows how to configure the default timeout values for hardware slowport monitoring:

```
switch(config)# system timeout slowport-monitor default mode F
switch(config)#
```

Related Commands

Command	Description
show process creditmon slowport-monitor-events	Displays the slowport monitor statistics information.

system timestamp format

To configure the uniform logging timestamp format, use the **system timestamp format** command. To remove this configuration, use the **no** form of this command.

system timestamp format rfc5424

Syntax Description

rfc5424	Specifies RFC 5424 compliant timestamps.

Command Default

Events are logged with mixed timestamp formats.

Command Modes

Configuration mode (config)

Command History

Release	Modification
8.4(1)	This command was introduced.

Usage Guidelines

The Uniform Timestamps feature affects:

- onboard syslog
- onboard accounting log
- various internal logs of NX-OS features

The **rfc5424** option specifies to use RFC 5424 compliant timestamps for logging. RFC 5424 defines the format of the complete syslog message, but part of it is the syslog timestamp format which is used by this option.

RFC 5424 compliant timestamps have the following structure:

```
yyyy-mm-ddThh:mm:ss[.mmm[uuu]][Z|{+|-}hh:mm]

    where:

    yyyy is the 4-digit year
    mm is the 2-digit month of the year
    dd is the 2-digit date of the month
    T is a literal T
    hh is the 2-digit hour of the day
    mm is the 2-digit minute of the hour
    .mmm is the 3-digit millisecond (optional)
    uuu is the 3-digit microsecond (optional)
    Z is a literal Z, used if UTC timezone is set (optional)
    + is a literal +, used if the timezone offset from UTC is positive (optional)
    - is a literal -, used if the timezone offset from UTC is negative (optional)
    hh is the 2-digit hour component of the timezone offset from UTC (optional)
    mm is the 2-digit minute component of the timezone offset from UTC (optional)
```

Some software features log messages with timestamps that cannot be converted between formats. In the logs of such features, it is possible to have a mixture of timestamp formats. Thus, messages logged before and

after the timestamp format change will have the format that was configured at the time the log message was generated.

Not all logs support all the optional fields.

This command does not change the format of syslogs that are exported to an external syslog server via the syslog protocol.

Examples

The following example displays how to configure RFC 5424 compliant timestamps:

```
switch# configure terminal
switch(config)# system timestamp format rfc5424
```

The following example displays how to return to the original NX-OS timestamp format:

```
switch# configure terminal
switch(config)# no system timestamp format rfc5424
```

The following example displays the original timestamp format in syslog:

```
switch# show logging logfile
2019 Mar  8 09:52:04 switch last message repeated 3 times
```

The following example shows RFC 5424 compliant timestamp with the default switch timezone (UTC timezone, which is shown as Z):

```
switch# show accounting log
2019-05-28T16:39:36Z:type=update:id=192.168.1.2@pts/0:user=admin:cmd=configure terminal ;
logging level all 7 (SUCCESS)
```

The following example shows RFC 5424 compliant timestamp with a timezone offset of +1 hour:

```
switch# show accounting log
2019-05-30T07:17:51+01:00:type=update:id=192.168.1.2@pts/0:user=admin:cmd=configure terminal
 ; interface mgmt0 ; ipv6 enable (SUCCESS)
```

The following example displays the original timestamp format of an FCNS internal log:

```
switch# show fcns internal event-history
1) Event:E_MTS_RX, length:60, at 104710 usecs after Fri May 31 07:56:23 2019
    [REQ] Opc:MTS_OPC_SDWRAP_DEBUG_DUMP(1530), Id:0X031AF189, Ret:SUCCESS
    Src:0x00000501/7442, Dst:0x00000501/19, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x031AF189, Sync:UNKNOWN, Payloadsize:216
    Payload:
    0x0000:  01 00 2f 74 6d 70 2f 64 62 67 64 75 6d 70 34 39
```

The following example displays the timestamp format of an FCNS internal log when RFC 5424 compliant timestamping is enabled:

```
switch# show fcns internal event-history
1) Event:E_MTS_RX, length:60, at 2019-05-15T07:54:19.129048-07:00
    [REQ] Opc:MTS_OPC_SDWRAP_DEBUG_DUMP(1530), Id:0X003CE5D3, Ret:SUCCESS
    Src:0x00000501/14615, Dst:0x00000501/19, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x003CE5D3, Sync:UNKNOWN, Payloadsize:216
    Payload:
    0x0000:  01 00 2f 74 6d 70 2f 64 62 67 64 75 6d 70 32 38
```

Related Commands

Command	Description
clock format show-timezone syslog	Configure logging of timezone information in syslogs.
logging timestamp	Configure syslog timestamp resolution.
show system timestamp format	Displays the logging timestamp format.

system trace

To configure the system trace level, use the **system trace** command in configuration mode. To disable this feature, use the **no** form of the command.

system trace *bit-mask*
no system trace

Syntax Description

bit-mask	Specifies the bit mask to change the trace level.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is used for debugging purposes.

Examples

The following example shows how to configure the system trace level:

```
switch# config terminal
switch(config)# system trace 0xff
```

system transceiver power-control

Use the **system transceiver power-control** command to automatically power off the transceiver if interface is in admin shutdown.

Use the **no** form of the command to disable the command.

system transceiver power-control

no system transceiver power-control

Syntax Description

power-control	Automatically powers off the transceiver if interface is in admin shutdown.

Command Default

Automatically powers off the transceiver if the interface is in an admin down (shutdown) state.

Command Modes

Global Configuration mode

Command History

Release	Modification
9.4(2)	This command was introduced.

Usage Guidelines

This feature applies only to 64 Gbps capable interfaces. All transceiver types are supported.

When you enable this feature and shut down a 64 Gbps capable interface, the system turns off power to the transceiver, reducing overall switch power consumption.

You can view the transceiver power status for an interface in the **show interface** and s**how interface transceiver details** command outputs. When the transceiver power is off all values will be displayed as *NA*.

When performing ISL diagnostic testing via the **diagnostic isl** or **system health isl** commands transceiver power-control should be off for the duration of the test.

Examples

The following command turns off transceiver power-control which will re-energize all the transceivers in 64 Gbps capable interfaces in admin down state.

```
switch# configure terminal
switch(config)# no system transceiver power-control
```

Related Commands

Command	Description
show interface	Displays interface settings and counters
show interface transceiver details	Displays detailed transceiver values.
show system transceiver power-control	Displays power control is on/off/not Supported.
system default	Configures system default values.

system watchdog

To enable watchdog checks, use the **system watchdog** command in EXEC mode. To disable this feature, use the **no** form of the command.

system watchdog
no system watchdog

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If a watchdog is not logged at every 8 seconds by the software, the supervisor module reboots the switch.

You can disable the watchdog checking feature (enabled by default) for debugging and troubleshooting purposes such as attaching a GDB or a kernel GDB (KGDB) to a specified process.

Examples

The following example enables the system watchdog:

```
switch# system watchdog
```