



CHAPTER 21

S Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See [“About the CLI Command Modes”](#) section on page 1-3 to determine the appropriate mode for each command.

Send documentation comments to mdsfeedback-doc@cisco.com

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

<i>salt</i>	Specifies the salt for encryption. The range is from 0x0 to 0xffffffff.
-------------	---

Defaults

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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
```

Send documentation comments to mdsfeedback-doc@cisco.com

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

Send documentation comments to mdsfeedback-doc@cisco.com

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

Defaults

Disabled.
The IO-timeout is 10 seconds.
Lun-size-handling is Enabled.

Command Modes

onfiguration mode.

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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-c1)# scaling batch enable
switch(config-sme-c1)#
```

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
<i>username</i>	(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.
<i>password</i>	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.
<i>job-name</i>	Specifies the name of the scheduler job. The maximum length is 31 characters.
logfile size	Specifies a log file configuration.
<i>filesize</i>	Specifies the size of the log file. The range is 16 to 1024 KB.
schedule name	Specifies a scheduler schedule.
<i>schedule-name</i>	Specifies the name of the schedule. The maximum length is 31 characters.

Defaults 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.

Send documentation comments to mdsfeedback-doc@cisco.com

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)#
```

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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

Defaults 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
```

Send documentation comments to mdsfeedback-doc@cisco.com

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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.

Defaults

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:

Send documentation comments to mdsfeedback-doc@cisco.com

```
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.

Send documentation comments to mdsfeedback-doc@cisco.com

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

<i>vsan-id</i>	Specifies the number of the VSAN. The range is 1 to 4093.
----------------	---

Defaults

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
NX-OS 5.0(1a)	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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

<i>vsan-id</i>	Specifies the number of the VSAN. The range is 1 to 4093.
----------------	---

Defaults

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
NX-OS 5.0(1a)	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Defaults Disabled.

Command Modes Configuration mode

Command History	Release	Modification
	NX-OS 5.0(1a)	This command was deprecated.
	NX-OS 4.1(1b)	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 virtual-device	Displays the virtual devices.

Send documentation comments to mdsfeedback-doc@cisco.com

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

Defaults Disabled.

Command Modes Configuration mode

Command History	Release	Modification
	NX-OS 5.0(1a)	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
```

Send documentation comments to mdsfeedback-doc@cisco.com

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

Send documentation comments to mdsfeedback-doc@cisco.com

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 <i>threshold</i>	Configures the recovery schema threshold. The limit is 2-3.
total <i>total</i>	Configures the recovery schema total. The limit is 5-5.

Defaults

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-c1)# security-mode basic
```

The following example sets the security mode to advanced:

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

Related Commands

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

Send documentation comments to mdsfeedback-doc@cisco.com

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	<i>message-text</i>	Specifies the text of your message.
---------------------------	---------------------	-------------------------------------

Defaults	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.
```

Send documentation comments to mdsfeedback-doc@cisco.com

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 address or DNS name*

Syntax Description	<i>ipaddress or DNS name</i> Specifies LDAP server name.				
Defaults	None.				
Command Modes	Configuration submode				
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>NX-OS 5.0(1a)</td><td>This command was introduced.</td></tr></table>	Release	Modification	NX-OS 5.0(1a)	This command was introduced.
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: <pre>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)#</pre>				
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ldap-server groups</td><td>Displays the configured LDAP server groups.</td></tr></table>	Command	Description	show ldap-server groups	Displays the configured LDAP server groups.
Command	Description				
show ldap-server groups	Displays the configured LDAP server groups.				

Send documentation comments to mdsfeedback-doc@cisco.com

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	<i>server-id</i> Specifies the server address. The format is <i>A.B.C.D</i> .
---------------------------	---

Defaults	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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

Defaults	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
	<code>show dmm ip-peer</code>	Displays job information.
	<code>show dmm srvr-vt-login</code>	Displays server VT login information.

Send documentation comments to mdsfeedback-doc@cisco.com

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

Defaults	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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-address* | *ipv6-address* | *dns-name*]

no server [*ipv4-address* | *ipv6-address* | *dns-name*]

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

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

Command Modes	RADIUS configuration submode
---------------	------------------------------

Command History	Release	Modification
	1.3(1)	This command was introduced.
	3.0(1)	Added the <i>ipv6-address</i> 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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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-address* | *ipv6-address* | *dns-name*]

no server [*ipv4-address* | *ipv6-address* | *dns-name*]

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

Defaults None.

Command Modes TACACS+ configuration submode

Command History	Release	Modification
	1.3(1)	This command was introduced.
	3.0(1)	Added the <i>ipv6-address</i> 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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

set (IPsec crypto map configuration submode)

To configure attributes for IPsec crypto map entries, use the **set** command in IPsec crypto 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-name | set-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.
<i>ip-address</i>	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 120 to 86400.
transform-set	Configures the transform set name or set name list.
<i>set-name</i>	Specifies a transform set name. Maximum length is 63 characters.
<i>set-name-list</i>	Specifies a comma-separated transform set name list. Maximum length of each name is 63 characters. You can specified a maximum of six lists.

Defaults

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

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Send documentation comments to mdsfeedback-doc@cisco.com

setup

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

setup

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

Defaults	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
```

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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: <pre>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</pre>
-----------------	---

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Defaults 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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
--------------------	-------	---

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

Command Modes	Interface configuration submenu
---------------	---------------------------------

Command History	Release	Modification
	1.0(1)	This command was introduced.

Usage Guidelines	The default state for interfaces is shutdown. Use the no shutdown command to enable an interface to carry traffic. When you try to shut down a management interface (mgmt0), a follow-up 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
```

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 submenu.
	show interface	Displays interface information.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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.

Send documentation comments to mdsfeedback-doc@cisco.com

shutdown (Cisco SME 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.
---------------------------	--

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

Command Modes	Cisco SME 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 cluster operation in order to start recovery:

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

Related Commands	Command	Description
	show sme cluster	Displays information about the Cisco SME cluster.

Send documentation comments to mdsfeedback-doc@cisco.com

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	<i>site-number</i> Identifies the unit to the outsourced throughput. Allows up to 256 alphanumeric characters in free format.	
Defaults	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.

Send documentation comments to mdsfeedback-doc@cisco.com

sleep

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

sleep {*seconds*}

Syntax Description	<i>seconds</i>	Specifies the delay in number of seconds. The range is 0 to 2147483647.
---------------------------	----------------	---

Defaults	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
	<i>name</i>	Identifies the cluster name.
	transport	Configures the transport information.
	ssl	Configures the transport SSL information.
	trustpoint	Configures the transport SSL trustpoint.
	<i>trustpoint label</i>	Identifies the trustpoint label.

Defaults 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)#
```

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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 <i>vsan-id</i>	Enables FICON on the specified VSAN.
	show ficon	Displays configured FICON details.

Send documentation comments to mdsfeedback-doc@cisco.com

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 <i>string</i>	Specifies SNMP community string. Maximum length is 32 characters.
group <i>group-name</i>	(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.
<i>name</i>	(Optional) Specifies the name of the contact. Maximum length is 80 characters.
location	Configures system location.
<i>location</i>	(Optional) Specifies system location. Maximum length is 80 characters.

Defaults

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
```

Send documentation comments to mdsfeedback-doc@cisco.com

Related Commands	Command	Description
	show snmp	Displays SNMP information.

Send documentation comments to mdsfeedback-doc@cisco.com

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	<i>line</i> (Optional) Modifies the system contact.	
Defaults	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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 <i>string</i>	SNMP community string.
	group <i>group-name</i>	(Optional) Group to which the community belongs.
Defaults	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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.
fsfpf	(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.

Send documentation comments to mdsfeedback-doc@cisco.com

Defaults

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
```

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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:
-----------------	---

<pre>switch# config t switch(config)# snmp-server enable traps entity fru switch(config)#</pre>

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

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.
---------------------------	--

Defaults	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.
---------------------------	--

Defaults	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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:
-----------------	---

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

Related Commands	Command	Description
	show snmp	Displays SNMP information.

Send documentation comments to mdsfeedback-doc@cisco.com

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 *host-address* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*]

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

Syntax Description

<i>host-address</i>	Specifies the name or IP address of the host (the targeted recipient).
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).
<i>community-string</i>	Sends a password-like community string with the notification operation.
udp-port <i>port</i>	(Optional) Specifies the port UDP port of the host to use. The default is 162.

Defaults

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
```

Send documentation comments to mdsfeedback-doc@cisco.com

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

Related Commands

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

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Defaults 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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

snmp-server user

To configure SNMP user information, use the **snmp-server user** command in 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

<i>username</i>	Specifies the user name. Maximum length is 32 characters.
<i>group-name</i>	(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.
<i>password</i>	(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.

Defaults

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Send documentation comments to mdsfeedback-doc@cisco.com

source

To configure a switched port analyzer (SPAN) source, use the **source** command in SPAN session configuration submode. To disable this feature, use the **no** form of the command.

```
source {filter vsan vsan-id | interface {fc slot/port [rx [traffic-type {initiator | mgmt | target}] |
tx [traffic-type {initiator | mgmt | target}] | traffic-type {initiator | mgmt | target}] |
fcip fcip-id | fv slot/dpp-number/fv-port | iscsi slot/port [rx [traffic-type {initiator | mgmt |
target}] | tx [traffic-type {initiator | mgmt | target}] | traffic-type {initiator | mgmt |
target}] | port-channel channel-number [rx [traffic-type {initiator | mgmt | target}] | tx
[traffic-type {initiator | mgmt | target}] | traffic-type {initiator | mgmt | target}] | sup-fc
number [rx [traffic-type {initiator | mgmt | target}] | tx [traffic-type {initiator | mgmt |
target}] | traffic-type {initiator | mgmt | target}]} |
vsan vsan-id}
```

```
no source {filter vsan vsan-id | interface {fc slot/port [rx [traffic-type {initiator | mgmt | target}] |
tx [traffic-type {initiator | mgmt | target}] | traffic-type {initiator | mgmt | target}] |
fcip fcip-id | fv slot/dpp-number/fv-port | iscsi slot/port [rx [traffic-type {initiator | mgmt |
target}] | tx [traffic-type {initiator | mgmt | target}] | traffic-type {initiator | mgmt |
target}] | port-channel channel-number [rx [traffic-type {initiator | mgmt | target}] | tx
[traffic-type {initiator | mgmt | target}] | traffic-type {initiator | mgmt | target}] | sup-fc
number [rx [traffic-type {initiator | mgmt | target}] | tx [traffic-type {initiator | mgmt |
target}] | traffic-type {initiator | mgmt | target}]} | vsan vsan-id}
```



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

filter	Configures SPAN session filter.
vsan <i>vsan-id</i>	Specifies the VSAN ID. The range is 1 to 4093.
interface	Specifies the interface type.
fc <i>slot/port</i>	(Optional) Specifies the Fibre Channel interface ID at a slot and port on an MDS 9000 Family switch.
fcip <i>fcip-id</i>	Specifies the FCIP interface ID. The range is 1 to 255.
fv <i>slot/dpp-number/fv-port</i>	Specifies a virtual F port (FV port) interface in the specified slot along with the data path processor (DPP) number and the FV port number.
iscsi <i>slot/port</i>	(Optional) Configures the iSCSI interface in the specified slot/port 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.
port-channel <i>channel-number</i>	Specifies the PortChannel interface ID. The range is 1 to 128.
sup-fc <i>number</i>	Specifies the inband interface, which is 0.
rx	(Optional) Specifies SPAN traffic in ingress direction.

Send documentation comments to mdsfeedback-doc@cisco.com

traffic-type	(Optional) Configures the SPAN traffic type.
initiator	(Optional) Specifies initiator traffic.
mgmt	(Optional) Specifies management traffic.
target	(Optional) Specifies target traffic.
tx	(Optional) Specifies SPAN traffic in egress direction.

Defaults

Disabled.

Command Modes

SPAN session configuration submode

Command History

Release	Modification
1.0(2)	This command was introduced.
3.1(2)	Added the interface bay ext option.

Usage Guidelines

None.

Examples

The following example shows how to create a SPAN session, then configures the SPAN traffic at all sources in VSAN 1:

```
switch# config terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

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

```
switch(config-span)# source vsan 1
```

The following example shows how to configure the SPAN source interface as PortChannel 1:

```
switch(config-span)# source interface port-channel 1
```

The following example shows how to configure the SPAN source interface as FC 9/1 with an egress filter for VSAN 1:

```
switch(config-span)# source interface fc9/1 tx filter vsan 1
```

The following example shows how to configure the SPAN source interface as FCIP 51:

```
switch(config-span)# source interface fcip 51
```

The following example shows how to configure the SPAN source interface as iSCSI interface 4/1:

```
switch(config-span)# source interface iscsi 4/1
```

The following example shows how to disable configure the SPAN source interface as FC 9/1 with an egress filter for VSAN 1:

```
switch(config-span)# no source interface fc9/1 tx filter vsan 1
```

Send documentation comments to mdsfeedback-doc@cisco.com

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

Send documentation comments to mdsfeedback-doc@cisco.com

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	<i>id</i> Specifies the SPAN max-queued-packets threshold ID. The range is 1 to 8191.							
Defaults	15.							
Command Modes	Configuration mode							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>3.3(1a)</td><td>This command was introduced.</td></tr></table>		Release	Modification	3.3(1a)	This command was introduced.		
Release	Modification							
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: <pre>switch# config Enter configuration commands, one per line. End with CNTL/Z. switch(config)# span max-queued-packets 1</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show span drop-counters</td><td>Displays the SPAN drop-counters.</td></tr><tr><td>show span max-queued-packets</td><td>Displays the SPAN max-queued-packets.</td></tr></table>		Command	Description	show span drop-counters	Displays the SPAN drop-counters.	show span max-queued-packets	Displays the SPAN max-queued-packets.
Command	Description							
show span drop-counters	Displays the SPAN drop-counters.							
show span max-queued-packets	Displays the SPAN max-queued-packets.							

Send documentation comments to mdsfeedback-doc@cisco.com

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*}

no span session {*session-id*}

Syntax Description	<i>session-id</i> Specifies the SPAN session ID. The range is 1 to 16.	
Defaults	None.	
Command Modes	Configuration mode	
Command History	Release	Modification
	1.0(2)	This command was introduced.
Usage Guidelines	None.	
Examples	The following example shows how to configure a SPAN session: <pre>switch# config terminal switch(config)# span session 1 switch(config-span)#</pre> The following example shows how to delete a SPAN session: <pre>switch(config)# no span session 1</pre>	
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.

Send documentation comments to mdsfeedback-doc@cisco.com

span session source interface

To configure the SPAN traffic in both ingress (rx) and egress (tx) directions, use the **span session source interface** command in Configuration mode.

span session *session-id* **source interface** *interface type*

Syntax Description	<i>session-id</i>	Specifies the SPAN session ID.
	<i>interface type</i>	Specifies the destination interface mapped to a Fiber Channel or FC tunnel.

Defaults None.

Command Modes Configuration mode

Command History	Release	Modification
	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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 <i>pwwn-id</i>	Specifies the peer WWN ID for special frames.
	profile-id <i>profile-number</i>	(Optional) Specifies the peer profile ID. The range is 1 to 255.

Defaults	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:
	<pre>switch# config terminal switch(config)# interface fcip 1 switch(config)# special-frame peer-wwn 11:11:11:11:11:11:11:11 switch(config)# special-frame peer-wwn 22:22:22:22:22:22:22:22 profile-id 10</pre>

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

Send documentation comments to mdsfeedback-doc@cisco.com

ssh

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

```
ssh {hostname | userid@hostname}
```

Syntax Description

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

Defaults

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:
```

Related Commands

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

Send documentation comments to mdsfeedback-doc@cisco.com

ssh key

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

ssh key {**dsa** [*bits*] | **rsa** [*bits*] | **rsa1** [*bits*]} [**force**]

no ssh key

Syntax Description	dsa <i>bits</i>	Generates a DSA key. The range for the number of bits is 768 to 1856.
	rsa <i>bits</i>	Generates an RSA key. The range for the number of bits is 768 to 2048.
	rsa1 <i>bits</i>	Generates an RSA1 key. The range for the number of bits is 768 to 2048.
	force	(Optional) Forces the generation of keys even when previous keys are present.

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

Command Modes	Configuration mode
---------------	--------------------

Command History	Release	Modification
	1.0(2)	This command was introduced.

Usage Guidelines	None.
------------------	-------

Examples	The following example shows how to generate an SSH key:
----------	---

```
switch# config terminal
switch(config)# ssh key rsa1 1024
generating rsa1 key.....
generated rsa1 key
switch(config)#
switch(config)# ssh key dsa 1024
generating dsa key.....
generated dsa key
switch(config)#
switch(config)# ssh key rsa 1024
generating rsa key.....
generated rsa key
switch(config)#
switch(config)# no ssh key
cleared RSA keys
switch(config)#
```

Send documentation comments to mdsfeedback-doc@cisco.com

Related Commands	Command	Description
	show ssh key	Displays SSH key information.
	ssh server enable	Enables SSH server.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.
---------------------------	--

Defaults	Disabled.
-----------------	-----------

Command Modes	Configuration mode
----------------------	--------------------

Command History	Release	Modification
	1.0(2)	This command was introduced.

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
--------------------	-----	--

Defaults	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-c1)# ssl kmc
```

Send documentation comments to mdsfeedback-doc@cisco.com

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	<i>string</i> Specifies the delayed time in seconds. The range is from 1 to 600.	
Defaults	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: <pre>switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)# ssm upgrade delay 500 switch(config)#</pre>	
Related Commands	Command	Description
	ssm enable feature	Enables the SCSI flow feature on the SSM.

Send documentation comments to mdsfeedback-doc@cisco.com

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 } | 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 <i>slot/port</i>	Specifies the Fiber Channel slot and port numbers.
node <i>slot</i>	Specifies the node number for partial provisioning of Storage Services Node card. The range is from 0 to 3 characters.
module <i>slot</i>	Specifies the SSM module slot number.
invista	Enables the Invista feature on the SSM.
bootflash: <i>uri</i>	Specifies the source location for internal bootflash with image name.
force	Forces an immediate configuration change.
module <i>slot-number</i>	Specifies the slot number of the SSM.
modflash: <i>uri</i>	Specifies the source location for internal modflash with image name.
slot0: <i>uri</i>	Specifies the source location for the CompactFlash memory or PC card with image name.
interface fc <i>slot/port</i>	Specifies the interface to be configured.
fc <i>slot/port</i>	Configures the Fibre Channel interface.
fc <i>slot/port-port</i>	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.

Defaults Disabled.

Command Modes Configuration mode

Send documentation comments to mdsfeedback-doc@cisco.com

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.
```

Send documentation comments to mdsfeedback-doc@cisco.com

```
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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.
<i>wwn-id</i>	Specifies the pWWN or nWWN ID.
system-assign	Generates the pWWN or nWWN value automatically.

Defaults

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 initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)# static nwwn system-assign
```

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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 <i>cmd-id</i>	Stops a specific SCSI command identified by the command number. The range is 0 to 2147483647.

Defaults	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:
	<pre>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</pre>

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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	<i>street-address</i>	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).
---------------------------	-----------------------	---

Defaults	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	Disabled.
-----------------	-----------

Command Modes	SPAN session configuration submode
----------------------	------------------------------------

Command History	Release	Modification
	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.

Send documentation comments to mdsfeedback-doc@cisco.com

Command	Description
source	Configures a SPAN source.
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.

Send documentation comments to mdsfeedback-doc@cisco.com

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*}

no switch-priority {*priority-value*}

Syntax Description	<i>priority-value</i>	Specifies the priority level. 0 is the highest priority and 7 the lowest.
---------------------------	-----------------------	---

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

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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		
	<i>wwn-id</i>	Specifies the port WWN, with the format <i>hh:hh:hh:hh:hh:hh:hh:hh</i> .
	autonomous-fabric-id <i>fabric-id</i>	Specifies the fabric ID for the IVR topology.
	vsan-ranges <i>vsan-range</i>	Specifies the IVR VSANs or range of VSANs. The range of values for a VSAN ID is 1 to 4093.
	default-autonomous-fabric-id <i>fabric-id</i>	Specifies the default fabric ID for the IVR topology.

Defaults 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 auto
switch(config)# autonomous-fabric-id database
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)# switch-wwn 28:1d:00:05:30:00:06:ea default-autonomous-fabric-id
16
```

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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	<i>name</i>	Specifies a switch name. Maximum length is 32 characters.
--------------------	-------------	---

Defaults	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).

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

switchport

To configure a switch port parameter on a Fibre Channel, Gigabit Ethernet, or management interface, use the **switchport** command in interface configuration submode. To discard the configuration, use the **no** form of the command.

Fibre Channel Interface

```
switchport {beacon | description text | encap eisl | fcbbbscn | fcrxbbscredit {credit [mode {E | Fx}]
| default | extended credit | performance-buffers {buffers | default}} | fcrxbuFSIZE size |
ignore {bit-errors} | mode {E | F | FL | Fx | NP | SD | ST | TL | auto} | owner {owner} |
rate-mode {dedicated | shared} | speed {1000 | 2000 | 4000 | auto [max 2000]} | trunk
{allowed vsan [{add] vsan-id | all} | mode {auto | off | on}}}
```

```
no switchport {beacon | description text | encap eisl | fcbbbscn | fcrxbbscredit {credit [mode {E |
Fx}] | default | extended credit | performance-buffers {buffers | default}} | fcrxbuFSIZE size |
| ignore {bit-errors} | mode {E | F | FL | Fx | NP | SD | ST | TL | auto} | owner {owner} |
rate-mode {dedicated | shared} | speed {1000 | 2000 | 4000 | auto [max 2000]} | trunk
{allowed vsan [{add] vsan-id | all} | mode {auto | off | on}}}
```

Gigabit Ethernet Interface

```
switchport {beacon | description text | mtu}
```

```
no switchport {auto-negotiate | beacon | description text | mtu | promiscuous-mode}
```

Management Interface

```
switchport {description text | duplex {auto | full | half} | speed {10 | 100 | 1000}}
```

```
no switchport {description text | duplex | speed}
```

Syntax	Description
beacon	Enables the beacon for the interface.
description <i>text</i>	Specifies the interface description. Maximum length is 80 characters.
encap eisl	Configures extended ISL (EISL) encapsulation for the interface.
fcbbbscn	Enables or disables buffer to buffer credit recovery.
fcrxbbscredit	Configures receive BB_credit for the port.
<i>credit</i>	Specifies receive BB_credit. The range is 1 to 255
mode	(Optional) Configures receive BB_credit for the specific port mode.
E	Configures receive BB_credit for E or TE port mode.
Fx	Configures receive BB_credit for F or FL port mode.
default	Configures default receive BB_credits depending on the port mode and capabilities.
extended <i>credit</i>	Specifies extended receive BB_credits. The range is 256 to 4095.
performance-buffers <i>buffers</i> default	Specifies receive BB_credit performance buffers. The range is 1 to 145. The default value is determined by a built-in algorithm.
fcrxbuFSIZE <i>size</i>	Specifies receive data field size for the interface. The range is 256 to 2112 bytes.
mode	Configures the port mode.

Send documentation comments to mdsfeedback-doc@cisco.com

E	Configures E port mode.
F	Configures F port mode.
FL	Configures FL port mode.
Fx	Configures Fx port mode.
NP	Configures NP port mode for N port virtualizer only.
SD	Configures SD port mode.
ST	Configures ST port mode.
TL	Configures TL port mode.
auto	Configures autosense mode.
owner	Configures the owner string on the port.
<i>owner</i>	Specifies the owner. The maximum length of the string is 80 characters.
rate-mode	Configures the rate mode for an interface.
dedicated	Specifies dedicated bandwidth for the port.
shared	Specifies shared bandwidth for the port.
speed	Configures the port speed.
1000	Configures 1000-Mbps speed.
2000	Configures 2000-Mbps speed.
4000	Configures 4000-Mbps speed.
auto	Configures autosense speed.
max 2000	(Optional) Configures 2-Gbps as the maximum bandwidth reserved in auto mode for 24-port and 48-port 4-Gbps switching module interfaces.
trunk	Configures trunking parameters on the interface.
allowed	Specifies the allowed list for interfaces.
vsan	Configures the VSAN range.
add	(Optional) Adds the VSAN ID to the range of allowed VSAN list.
<i>vsan-id</i>	Specifies the VSAN ID. The range is 1 to 4093.
all	Adds all the VSANs to allowed VSAN list.
off	Disables the trunking mode.
on	Enables the trunking mode.
mtu	Configures the maximum transmission unit (MTU) for the port.
off	Disables promiscuous mode.
on	Enables promiscuous mode.
duplex	Configures the port duplex mode.
auto	Configures auto negotiate duplex mode.
full	Specifies full duplex mode.
half	Configures half duplex mode.
10	Configures 10-Mbps port speed.
100	Configures 100-Mbps port speed.
1000	Configures 1000-Mbps port speed.

Defaults

The beacon is disabled.

Send documentation comments to mdsfeedback-doc@cisco.com

The EISL encapsulation is disabled.

The default receive data buffer size is 2112 bytes.

The port mode is **auto**.

The speed is **auto**.

The maximum auto speed is **2000**.

The trunk mode is **on**.

During ISSU for the operationally non trunking up ports, the admin trunk mode is changed to **off** to avoid network disruption due to mis-behaving devices in the network.

The rate mode is **shared**.

Command Modes

Interface configuration submode

Command History

Release	Modification
NX-OS 4.1(3)	Added the F and NP port mode.
1.0(2)	This command was introduced.
2.0(1b)	Added the extended option to the fcrxbbcredit keyword.
3.0(1)	- Added the fcbbscn option. - Added the ST option to the mode keyword. - Added the 4000 option to the speed keyword. - Added the auto max 2000 option to the speed keyword. - Added the rate-mode keyword. - Added the Gigabit Ethernet interface syntax. - Added the management interface syntax.

Usage Guidelines

You can specify a range of interfaces by entering a command with the following example format:

interfacespacefc1/1space-space5space,spacefc2/5space-space7



Tip

The **shutdown** or **no shutdown** command for the FCIP or iSCSI interfaces is automatically entered when you change the MTU size—you do not need to explicitly enter this command.

You must perform the **fcrxbbcredit extended enable** command in configuration mode to use the **switchport fcrxbbcredit extended** command in interface configuration submode to enable extended BB_credits on a Fibre Channel interface.

The port speed on an interface, combined with the rate mode, determines the amount of shared resources available to the ports in the port group. Especially in the case of dedicated rate mode, the port group resources are reserved even though the bandwidth is not used. For example, if an interface is configured for autosensing (**auto**), then 4 Gbps of bandwidth is reserved even though the maximum operating speed is 2 Gbps. For the same interface, if autosensing with a maximum speed of 2 Gbps (**auto max 2000**) is configured, then only 2 Gbps of bandwidth is reserved and the unused 2 Gbps is shared with the other interface in the port group.

Send documentation comments to mdsfeedback-doc@cisco.com

**Note**

The 4-port 10-Gbps switching module only supports 10-Gbps traffic.

Table 21-1 lists the default configurations, credits, and buffers for switching modules.

Table 21-1 **Default Configurations, Credits, and Buffers**

Switching Module	Speed	Port Mode	Rate Mode	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 E-port	Dedicated Dedicated	2/250/16 2//250/250
DS-C9222i-K9, Cisco MDS 9222i Switch	1-, 2-, or 4-Gbps	Fx	Shared	1/16/16
		Fx E-port	Dedicated Dedicated	2/250/16 2//250/250
DS-X9704, Cisco MDS 9000 Family 4-Port 10-Gbps Fibre Channel Switching Module	10-Gbps	NA	Shared	NA
		Fx E-port	Dedicated Dedicated	2/750/16 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 E-port	Dedicated Dedicated	2/250/32 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 E-port	Dedicated Dedicated	2/500/32 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 E-port	Dedicated Dedicated	2/500/32 2/500/500
DS-C9148-K9, Cisco MDS 9148 48-Port Multilayer Fabric Switch	1-, 2-, 4-, or 8-Gbps	NA	Shared	NA
		Fx E-port	Dedicated Dedicated	1/125/32 1/125/32
DS-C9134-K9, Cisco MDS 9134 34-Port Multilayer Fabric Switch	1-, 2-, or 4-Gbps	NA	Shared	NA
		Fx E-port	Dedicated Dedicated	1/61/16 1/61/16
DS-C9124-K9, Cisco MDS 9124 24-Port Multilayer Fabric Switch	1-, 2-, or 4-Gbps	NA	Shared	NA
		Fx E-port	Dedicated Dedicated	1/61/16 1/61/16

When configuring port modes, observe the following guidelines:

Send documentation comments to mdsfeedback-doc@cisco.com

- Auto port mode and E port mode cannot be configured in shared rate mode.
- The 4-port 10-Gbps module does not support FL port mode.
- Generation 2 modules do not support TL port mode.
- Shared to dedicated ports should be configured in this order: speed, rate mode, port mode, credit.
- Dedicated to shared ports should be configured in this order: credit, port mode, rate mode, speed.

When configuring PortChannels, observe the following guidelines:

- When an interface is out-of-service, it cannot be part of a PortChannel.
- 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 PortChannels for Generation-2 modules is 256.
- The maximum number of PortChannels for a mixture of Generation-1 and Generation-2 modules is 128.
- The number of PortChannels is independent of the type of supervisor module.
- When adding a PortChannel to a configuration that uses both Generation-1 and Generation-2 modules, configure the PortChannel and Generation-2 interface speed to **auto max 2000**.
- When using the force option to add a PortChannel to a configuration that uses both Generation-1 and Generation-2 modules, follow these guidelines:
 - Configure the PortChannel interface speed to **auto max 2000**, or add the Generation-1 interfaces followed by the Generation-2 interfaces.
 - Generation-1 interfaces do not support the **auto max 2000** speed.
 - The force addition can fail for a Generation-2 interface if resources are unavailable.

Examples

The following example shows how to configure NP port mode:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface fc 1/1
switch(config-if)# switchport mode NP
fc1/1: (error) port already in a port-channel, no config allowed
switch(config-if)#
```

The following example shows how to enable buffere-to-buffer credit recovery on the interface:

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

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

```
switch(config-if)# no switchport fcbbscn
```

The following example configures switch port parameters for a Fibre Channel interface:

```
switch# config terminal
switch(config)# interface fc 1/23
switch(config-if)# switchport description techdocsSample
switch(config-if)# switchport mode E
switch(config-if)# switchport trunk mode auto
switch(config-if)# switchport trunk allowed vsan all
```

Send documentation comments to mdsfeedback-doc@cisco.com

```
switch(config-if)# switchport trunk allowed vsan 3
switch(config-if)# switchport trunk allowed vsan add 2
switch(config-if)# switchport encap eisl
switch(config-if)# switchport fcrxbbcredit performance-buffers 45
switch(config-if)# switchport proxy-initiator nWWN 11:11:11:11:11:11:11:11 pwnn
22:22:22:22:22:22:22:22
switch(config-if)# no switchport proxy-initiator nWWN 11:11:11:11:11:11:11:11 pwnn
22:22:22:22:22:22:22:22
switch(config-if)# switchport fcrxbbcredit extended 2000
```

The following example configures the port speed of a Fibre Channel interface and enables autosensing on the interface:

```
switch# config terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport speed 4000
switch(config-if)# switchport speed auto
```

The following example reserves dedicated bandwidth for the interface:

```
switch(config-if)# switchport rate-mode dedicated
```

The following example reserves shared (default) bandwidth for the interface:

```
switch(config-if)# switchport rate-mode shared
```

Related Commands

Command	Description
fcrxbbcredit extended enable	Enables extended BB_credits on the switch.
show interface	Displays an interface configuration for a specified interface.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

switchport auto-negotiate

To configure auto-negotiation on Gigabit Ethernet interfaces, use the **switchport auto-negotiate** command in configuration mode. Use the **no** form of the command to delete the configured switch port information.

switchport auto-negotiate

no switchport auto-negotiate

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

Defaults	Enabled.
-----------------	----------

Command Modes	Interface configuration submode
----------------------	---------------------------------

Command History	Release	Modification
	1.1(1)	This command was introduced.

Usage Guidelines	You can configure the auto-negotiate option for a specified Gigabit Ethernet interface. By default, the port is configured to auto-negotiate. By configuring auto-negotiation, the port automatically detects the speed or pause method and duplex of incoming signals and synchronizes with them.
-------------------------	--

Access this command from the switch(config-if)# submode for Gigabit Ethernet interfaces.

Examples	The following example configures auto-negotiation on a Gigabit Ethernet interface:
-----------------	---

```
switch# config t
switch(config)# interface gigabitethernet 8/1
switch(config-if)# switchport auto-negotiate
```

The following example disable auto-negotiation on a Gigabit Ethernet interface:

```
switch(config-if)# no switchport auto-negotiate
```

Related Commands	Command	Description
	show interface gigabitethernet	Displays an interface configuration for a specified Gigabit Ethernet interface.

Send documentation comments to mdsfeedback-doc@cisco.com

switchport ignore bit-errors

To prevent the detection of bit error threshold events from disabling the interface on Fibre Channel interfaces, use the **switchport ignore bit-errors** command. To revert to the default, use the **no** form of the command.

switchport ignore bit-errors

no switchport ignore bit-errors

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

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

Command Modes	Interface configuration submenu
----------------------	---------------------------------

Command History	Release	Modification
	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. You can enter a **shutdown/no shutdown** command sequence to reenable the interface.



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 the interface:
-----------------	--

Send documentation comments to mdsfeedback-doc@cisco.com

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

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

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# no switchport ignore bit-errors
```

Related Commands

Command	Description
show interface	Displays interface information.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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	<i>limit</i> Specifies the ingress rate limit as a percentage. The range is 1 to 100.	
Defaults	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: <pre>switch# config terminal switch(config)# interface fc 2/5 switch(config-if)# switchport ingress-rate 5</pre>	
Related Commands	Command	Description
	show interface fc	Displays an interface configuration for a specified Fibre Channel interface.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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-address* | *name*}

no switchport initiator id {*ip-address* | *name*}

Syntax Description

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

Defaults

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.

Send documentation comments to mdsfeedback-doc@cisco.com

switchport owner

To configure the owner string on the port, use the **switchport owner** command. To disable this feature, use the **no** form of the command.

switchport owner [*owner*]

no switchport owner

Syntax Description	<i>owner</i>	(Optional) Specifies the owner. The maximum length of the string is 80 characters.
--------------------	--------------	--

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

Command Modes	Interface Configuration mode
---------------	------------------------------

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 the port:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch (config)# interface fc1/1
Switch (config-if)# switchport owner used_by_fc_admin
switch(config-if)#
```

The following example shows how to remove the owner string from the port:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch (config)# interface fc1/1
Switch (config-if)# no switchport owner
```

Related Commands	Command	Description
	show interface	Displays an interface configuration for a specified interface.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

switchport promiscuous-mode

To configure the promiscuous-mode in Gigabit Ethernet interfaces, use the **switchport promiscuous-mode** command in interface configuration submode. Use the **no** form of the command to delete the configured switch port information.

switchport promiscuous-mode {off | on}

no switchport promiscuous-mode

Syntax Description	off	Disables promiscuous mode.
	on	Enables promiscuous mode.

Defaults	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 for Gigabit Ethernet interfaces.
------------------	--

Examples	The following example enables promiscuous mode on a Gigabit Ethernet interface:
----------	---

```
switch# config terminal
switch(config)# interface gigabitethernet 8/1
switch(config-if)# switchport promiscuous-mode on
```

The following example disables promiscuous mode on a Gigabit Ethernet interface:

```
switch(config-if)# switchport promiscuous-mode off
```

The following example disables promiscuous mode on a Gigabit Ethernet interface:

```
switch(config-if)# no switchport promiscuous-mode
```

Related Commands	Command	Description
	show interface gigabitethernet	Displays an interface configuration for a specified Gigabit Ethernet interface.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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 <i>wwn</i>	(Optional) Specifies the node WWN.
pwwn <i>wwn</i>	(Optional) Specifies the port WWN.

Defaults

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
```

Send documentation comments to mdsfeedback-doc@cisco.com

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

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Defaults

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.	
Defaults	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:	
	<pre>switch(config)# system delayed-traps enable mode FX switch(config)#</pre>	

Send documentation comments to mdsfeedback-doc@cisco.com

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	<i>number</i>	Indicates the delayed trap timer in minutes. The range is from 1 to 60.
---------------------------	---------------	---

Defaults	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)#
```

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

system default interface congestion timeout

To configure the default timeout value for a congestion timeout, use the **system default 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

<i>milliseconds</i>	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.

Defaults

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)#
```

Send documentation comments to mdsfeedback-doc@cisco.com

Related Commands	Command	Description
	show interface brief	Displays FC port modes.
	show system default switchport	Displays default values for switch port attributes.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

system default interface congestion mode

To configure the default interface congestion mode, use the **system default interface congestion mode** 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.
Defaults	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:	
	<pre>switch# config terminal switch(config)# system default interface congestion mode core switch(config)#</pre>	
	The following example shows how to disable the default interface congestion mode for the edge port type:	
	<pre>switch# config terminal switch(config)# no system default interface congestion mode edge switch(config)#</pre>	
Related Commands	Command	Description
	show interface brief	Displays FC port modes.
	show system default switchport	Displays default values for switch port attributes.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

system default interface pause timeout

To configure the default timeout value for a pause frame, use the **system default interface 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	<i>milliseconds</i>	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.

Defaults 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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

system default interface pause mode

To configure the default timeout value for a pause frame, use the **system default interface pause 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.

Defaults

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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 F}

no system default switchport {shutdown | trunk mode {auto | off | on} | mode 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 F	Sets the administrative mode of Fibre Channel ports to mode F.

Defaults	Enabled.
-----------------	----------

Command Modes	Configuration mode
----------------------	--------------------

Command History	Release	Modification
	1.0(2)	This command was introduced.
	3.1(3)	Added the mode F option.

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
```

Send documentation comments to mdsfeedback-doc@cisco.com

```
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
```

Related Commands

Command	Description
show interface brief	Displays FC port modes.
show system default switchport	Displays default values for switch port attributes.

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Defaults 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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.
---------------------------	--

Defaults	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
```

Send documentation comments to mdsfeedback-doc@cisco.com

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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.

Defaults

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)#
```

Send documentation comments to mdsfeedback-doc@cisco.com

Related Commands	Command	Description
	show system default zone	Displays the zone specific system default value settings.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.

Defaults

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
--------------------	--------	---

Defaults	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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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
-----------------	--

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Defaults

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.
3.1(2)	Added the interface bay ext option.

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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 <i>slot</i>	Specifies the module slot number.
--------------------	---------------------------	-----------------------------------

Defaults	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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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 <i>slot</i>	Specifies the module slot number.
---------------------------	-----------------------------------

Defaults

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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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 slot/port* | *iscsi slot/port*}

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 configure on 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.

Defaults

Enabled.

Command Modes

EXEC mode.

Send documentation comments to mdsfeedback-doc@cisco.com

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
```

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.

Defaults

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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.

Defaults

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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

<i>slot</i>	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 <i>seconds</i>	(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.

Defaults

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

Send documentation comments to mdsfeedback-doc@cisco.com

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:

Send documentation comments to mdsfeedback-doc@cisco.com

```
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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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]
```



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	(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.

Defaults

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
```

Send documentation comments to mdsfeedback-doc@cisco.com

```
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.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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
```

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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
```

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

system startup-config

To release a system startup configuration lock, use the **system startup-config** command in EXEC mode.

system startup-config unlock *lock-id*

Syntax Description	unlock <i>lock-id</i>	Configures the system startup-config unlock ID number. The range is 0 to 65536.
--------------------	------------------------------	---

Defaults	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 <i>lock-id</i> , use the show system internal sysmgr startup-config locks command.
------------------	--

Examples	The following example releases the system configuration lock with identifier 1: switch# system startup-config unlock 1
----------	--

Related Commands	Command	Description
	show system	Displays system information.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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
```

Send documentation comments to mdsfeedback-doc@cisco.com

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

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes EXEC mode

Command History	Release	Modification
	1.3(1)	This command was introduced.

Usage Guidelines Any switchover function is nonrevertive. Once a switchover has occurred and the failed processor has been replaced or successfully restarted, you cannot switch back to the original, active supervisor module (unless there is a subsequent failure or you issue the **system switchover** command).

Examples The following example initiates a HA switchover from an active supervisor module to a standby supervisor module:

```
switch# system switchover
```

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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

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* **mode** E/F | **default mode** E/F

Syntax Description	<i>number</i>	Number in milliseconds. The range is fom 100 to 1000 milliseconds.
	default	Specifies the default timeout values for congestion drop.
	mode	Specifies the Port mode.
	E	Specifies the E mode.
	F	Specifies the F mode.

Defaults 500 ms.

Command Modes Global configuration mode

Command History	Release	Modification
	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 mode E:

```
switch(config)# system timeout congestion-drop 110 mode E
switch(config)# timeout for mode F should be smaller than mode E.
switch(config)#
```

The following example shows how to configure the default timeout values for congestion drop E mode:

```
switch(config)# system timeout congestion-drop default mode E
switch(config)#
```

Related Commands	Command	Description
	system timeout no-credit-drop	Configures the system timeout values for no credit drop.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

system timeout no-credit-drop

To configure the system timeout values for no credit drop, use the **system timeout no-credit-drop** command.

system timeout no-credit-drop *number* **mode** E/F | **default mode** E/F

Syntax Description	<i>number</i>	Number in milliseconds. The range is from 100 to 1000 milliseconds.
	default	Specifies the default timeout values for no credit drop.
	mode	Specifies the Port mode.
	E	Specifies the E mode.
	F	Specifies the F mode.

Defaults	Disabled.
-----------------	-----------

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

Command History	Release	Modification
	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.
-------------------------	--

Examples	The following example shows how to configure the system timeout values for no credit drop F mode:
-----------------	---

```
switch(config)# system timeout no-credit-drop 100 mode F
switch(config)#
```

The following example shows how to configure the default timeout values for no credit drop F mode:

```
switch(config)# system timeout no-credit-drop default mode F
switch(config)#
```

Related Commands	Command	Description
	system timeout congestion-drop	Configures the system timeout values for congestion drop.

Send documentation comments to mdsfeedback-doc@cisco.com

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.
Defaults	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	

Send documentation comments to mdsfeedback-doc@cisco.com

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	<i>bit-mask</i>	Specifies the bit mask to change the trace level.
---------------------------	-----------------	---

Defaults	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: <pre>switch# config terminal switch(config)# system trace 0xff</pre>
-----------------	--

Send documentation comments to mdsfeedback-doc@cisco.com

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.
---------------------------	--

Defaults	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: <pre>switch# system watchdog</pre>
-----------------	---

Send documentation comments to mdsfeedback-doc@cisco.com